digit Fast Track to SECURITY

// Initialize DB-Library.
dbinit ();
a:link{color:#
dbsqlexec
a:active,.q:active,.q:visited{color:#20c
}a:active{color:red}.cur{color:#a90a08;f

- Personal Computer
- The Internet
- Cybercafes
- Laptops
- Portable devices
- Mobile phones

YOUR HANDY GUIDE TO EVERYDAY TECHNOLOGY

Fast Track to

Security

By Team Digit

digit FAST TRACK

FAST TRACK

Credits

The People Behind This Book

EDITORIAL

Editor-in-chief	**Edward Henning**
Editor	**Robert Sovereign-Smith**
Head-Copy Desk	**Nash David**
Writer	**Ravi Sinha, Aditya Madanapalle, Nash David**

DESIGN AND LAYOUT

Layout Design	**Vijay Padaya**
Cover Design	**Kabir Malkani**

Published by 9.9 Interactive

July 2009

Free with Digit. Not to be sold separately. If you have paid separately for this book, please email the editor at **editor@thinkdigit.com** along with details of location of purchase, for appropriate action.

CONTENTS

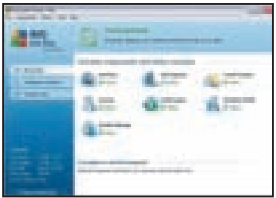
1: Personal Computer

1.1 Anti-Virus

Viruses are the bane of many a PC user's existence. They can attack you through malicious web sites, corrupt important system files and even erase important data. However, you can keep yourself safe with anti-virus software. Anti-virus software comes in several types of packages – best of all, some of the most effective anti-virus tools are freeware. Virus detection can also be achieved through online checks. It is imperative to understand their necessity, especially since they can slow down system performance and prompt the user with unfamiliar commands.

Normally, anti-virus software has three modes of detection:

1. Signature based detection – The most common method. It matches the contents of any infected files against a data base of virus signatures that are updated on a regular basis. This mode even examines files in pieces to detect the infected areas. However, constant updating of virus database definitions is essential.



AVG Free is one of the most reliable anti viruses around

2. Malicious activity detection – Monitors your system for suspicious behaviour. In case any suspicious activity is detected, the system initiates signature based detection. This is useful for catching unknown viruses that may not be listed in the database.

3. Heuristic based detection – The most system taxing mode of detection but the most effective for detecting unknown viruses. This is done through two methods: File analysis and file emulation. In file analysis, virus-like instructions that may be embedded in different programs rather than suspicious behaviour is investigated. If a program has instructions to format the C drive, for example, the anti-virus examines this program more closely. File emulation involves executing a program in a virtual environment and logging the actions that occur, according to which the anti-virus takes

appropriate disinfection measures. As stated however, both methods of this detection requires large amount of system resources.

One of the most reliable anti-virus solutions available is AVG Free. It's divided into three sections: Overview, Computer Scanner and Update Now. Overview provides info on the version running, last scan performed and the last definitions update. It also showcases all the option available like Link Scanner, E-mail Scanner, etc. and easily indicates whether they are up-to date (green) or outdated (red) along with their active status. If outdated, clicking on an option provides solutions.

Computer Scanner allows you to edit scan settings for the entire computer or specific folders and files. Scan settings let you determine scan access priority (fast, automatic or slow), the use of heuristics, automatically healing/removing infections and more. Scans can be also scheduled to run at specific times, on start-up or even after every few hours.

The Update Now section is the most straightforward tab. It automatically connects online to fetch the latest virus database definitions for detecting matching virus signatures.

For more options, click on `Tools > Advanced settings`. You can schedule scans for different components on the basis of frequency, time of day and what not. You can also determine update priorities, proxy settings, types of file extensions to be detected by the Resident Shield, etc.

On short notice at any time, free anti-virus scans are also available online through several reliable sites such as:

- **http://www.kaspersky.com/virusscanner**
- **http://security.symantec.com**
- **http://us.mcafee.com/root/mfs/scan.asp?affid=56**
- **http://www.bitdefender.com/scan8**
- **http://onecare.live.com/site/en-us/default.htm**
- **http://ca.com/securityadvisor/virusinfo/scan.aspx**
- **http://www.ewido.net/en/onlinescan**
- **http://www.pandasecurity.com/homeusers/solutions/activescan**

Some essential tips to preventing virus infections: Always scan external media. Schedule daily scans and updates (at the minimum). Never ever execute files from unknown email senders or follow unfamiliar links.

1.2 Anti-spyware

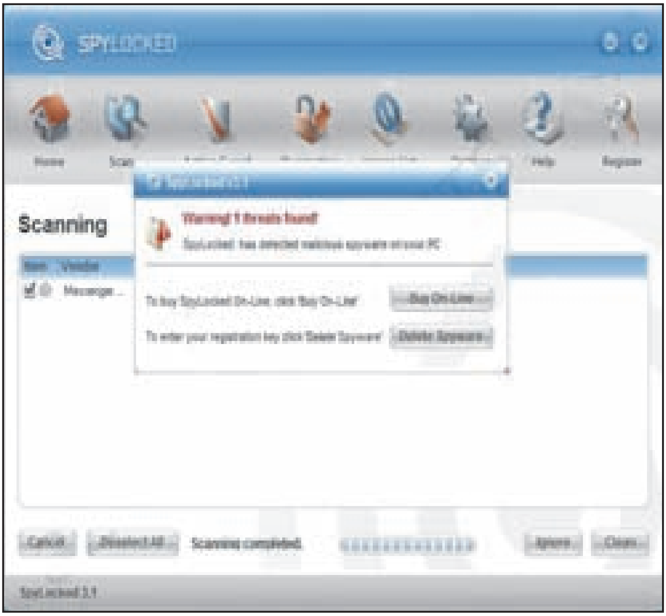
Judging from its name, you'd assume spyware was simply malware that monitors your PC activities. Spyware indeed collects personal information regarding what sites you visit and for how long. However, it can also wrest control from the user. It redirects one's browser activity and even permits the installation of additional software without one's consent or knowledge. Spyware doesn't infect neighbouring computers; it attacks by exploiting software loopholes. Some of its other more damaging effects include:

- Higher CPU utilisation
- Unwanted disk usage
- System crashes
- Software freezing
- Start-up failures
- Lower connection speeds

Spyware has several routes of infection. A common method is by "piggy-backing" on software downloads (such as Kazaa and Limewire). It can also come bundled with shareware. Keep in mind that the download itself is still safe, once the software is installed the spyware will be as well. Spyware authors often repackage popular freeware with installers for spyware.

Browsers such as Internet Explorer prevent any downloads from taking place without the user's permission. Through security holes in the web browser, certain web pages can override this and install spyware on the user's PC. This has come to be known as "drive-by download" since the user is helpless during the attack. It should be noted that later versions of IE have amended these loopholes.

Certain freeware "anti-spyware" programs can also contain spyware. There are currently over 300 listed applications. Such programs are classified as "rogue" anti-spyware programs. Examples of such malicious programs are Spy Wiper, WorldAntiSpy, Spylocked and Antivirus Gold. Many web pages associated with Adware Report, e-Spyware, NonToxic-Internet and others also come under rogue/suspect anti-spyware sites.



Warning! 1 threats found!

SpyLocked has detected malicious spyware on your PC

To buy SpyLocked On-Line, click 'Buy On-Line'

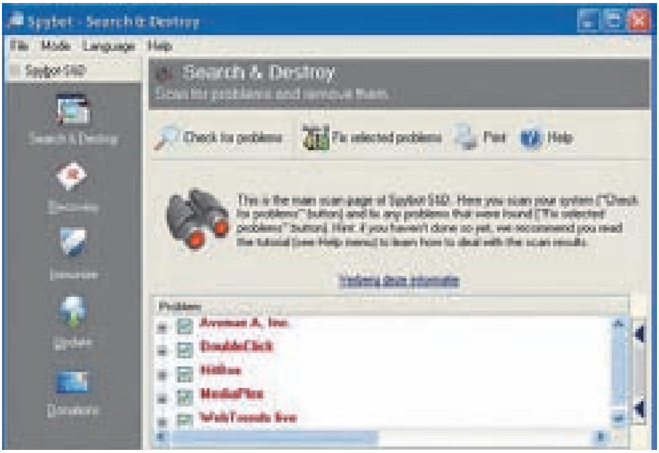
To enter your registration key click 'Delete Spyware'

Scanning completed.

Beware of "rogue" anti-spyware programs that contain infections

Finally, spyware can be delivered via viruses and worms as payload. For example, the Spybot worm causes several pornographic pop-ups to appear on the user's screen. This directs traffic and channels funds to the spyware authors.

The most common effect of spyware is the incidence of pop up ads. These are advertisements that appear in a separate window of the browser without the active consent of the user. They are the result of the spyware gathering info on the user. This feedback results in ads specifically targetted at the user depending on the sites browsed. Rootkits are newer and more powerful types of spyware. They can hide inside system critical processes such as Safe Mode, and are harder to detect since they leave no on-disk signatures. Newer spyware programs have countermeasures against anti-malware programs, such as preventing installation/execution of the same and even uninstalling them. Gromozon is one such malware



This is the main scan page of Spybot S&D. Here you scan your system ("Check for problems" button) and fix any problems that were found ("Fix selected problems" button). Hint: if you haven't done so yet, we recommend you read the tutorial (see Help menu) to learn how to deal with the scan results.

Use Spybot S&D to kill all that bad, bad spyware

that uses alternate data streams to hide. Coupled with a rootkit, it can escape alternate data stream scanners and prevent rootkit scanners from running.

Spyware can best be defined as junk that weighs down the PC. If accumulated for a long time, eventually the computer has to be formatted and software reinstalled to regain its former speeds. A strong anti-spyware solution should be in place and regular scans conducted to eliminate spyware before it accumulates. Spybot: Search and Destroy is one of the most popular and effective anti-spyware programs available. It detects keyloggers, rootkits, tracking cookies, ActiveX objects, homepage hijackers and even some trojans. It can also create a back-up registry to repair damaged files and restore them to their state prior to infection. Spybot's "Immunize" blocks the installation of the spyware before it happens by modifying its host file and a file shredder for secure deletion of files. The TeaTimer module provides active, real-time protection and alerts the user to any dangerous registry changes.

Spybot: S&D is commercially free, and its weekly updates add new features to keep pace with the latest threats while improving previous heuristic algorithms.

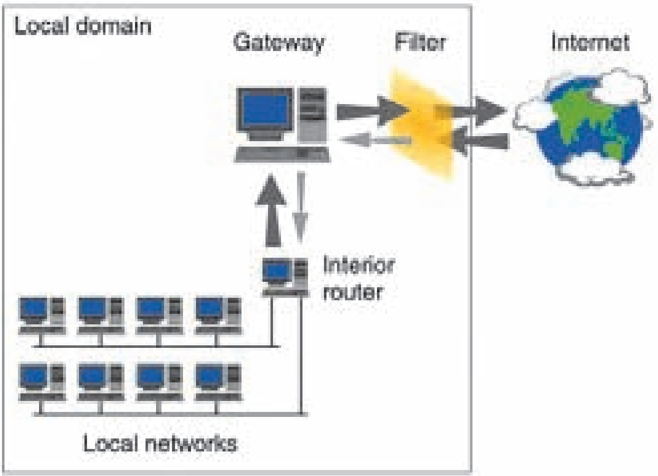
1.3 Firewalls

The internet is a gateway to sending and receiving limitless information. Like most gates, it has its share of intruders. And hence we have the gatekeepers – firewalls.

A firewall is part of a computer system or network designed to prevent unauthorised access while allowing verified and safe communications. It usually consists of a device or set of devices. It can also be implemented via hardware or software, or often a combination of both. Firewalls are most commonly used to prevent unauthorised internet users from accessing private networks, especially intranets. Each firewall has a different kind of authorisation criteria. Information entering or leaving the network through firewall that doesn't meet this standard is blocked.

Firewall techniques consist of four main types:

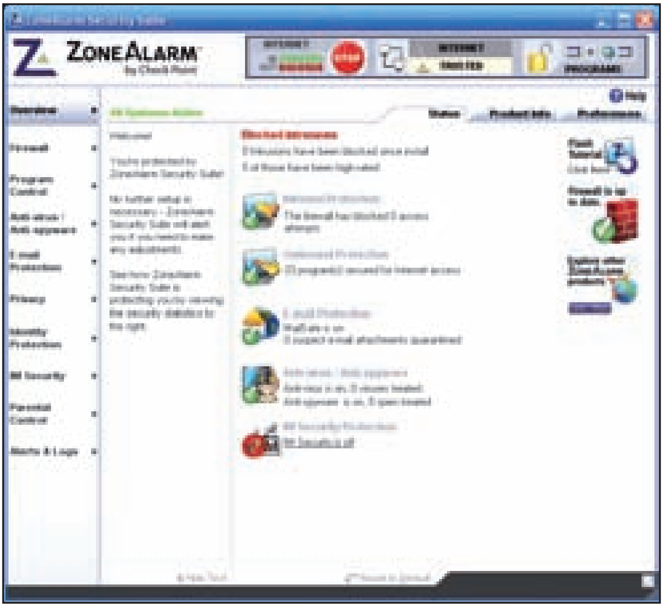
1. Packet filter: Packets are the most basic unit of data transfer between computers and networks. A packet filter uses a set of user defined rules for identifying the source, destination address, protocol and port number. If a particular packet matches the rules, the filter either discards it or rejects it (also drops the packet, but sends



an error response to the source). Fairly effective and transparent, packet filters are nonetheless tough to configure. They're also susceptible to IP spoofing wherein packets with forged IP addresses are created to either impersonate an "accepted" source or conceal the identity of the sender.

2. Application gateway: Also referred to as application proxies, they are located between the end user and network. The end user directly contacts the gateway, after which it performs requested function for the user. Specific programs use specific mechanisms. It is however not transparent to users, who must install custom applications to contact the gateways. This type is simple, since it only functions to proxy requests from end users. It also intercepts IP packets from the net. However, it causes strain on system performance.
3. Stateful firewall: It keeps track of the network connections moving across it (TCP streams, for example). It distinguishes legitimate packets for different connections and only allows packets matching a specific connection state. All others will be rejected. Sessions without traffic for a specific period will eventually time out to prevent the table from being filled. Stateful firewalls are advantageous as opposed to packet filters since it need only check the connection against its table rather than an extensive rule-set.
4. Proxy server: "Proxy" meaning "substitute". One of the more popular types, proxy servers act as go-betweens for outside clients seeking information from servers. The request is filed and checked according to various filtering rules hence filtering traffic from certain IP addresses. Direct access to the server is subsequently handled by the proxy on behalf of the client. It may speed up resource management by caching and delivering responses according to specific requests. The servers are hence kept anonymous and safe from attack.

An easy-to-use and powerful firewall can be found in ZoneAlarm, the newest release being ZoneAlarm Security Suite 2009. Besides an inbound intrusion detection system, it can also control which programs can make outbound



ZoneAlarm firewall can keep you safe in the ways shown above

connections. ZoneAlarm does this by dividing access into two "zones". There's the trusted zone, which includes computers and devices such as printers connected by LAN. Then there's the "internet zone". The user must manually specify permissions to give to a program before it tries to access the internet. ZoneAlarm may also prompt the user for permission the first time the program attempts net access.

A freeware version is available, but there's plenty of incentive to purchase the full versions. These are the OSFirewall and SmartDefense Advisor features. OSFirewall is present in all paid versions and monitors programs for suspicious behaviour. SmartDefense is only featured in the premium versions. It uses a large database of reliable program signatures to guide users with respect to allowing or denying program access to the internet. Different versions of ZoneAlarm also provide protection against viruses and spyware.

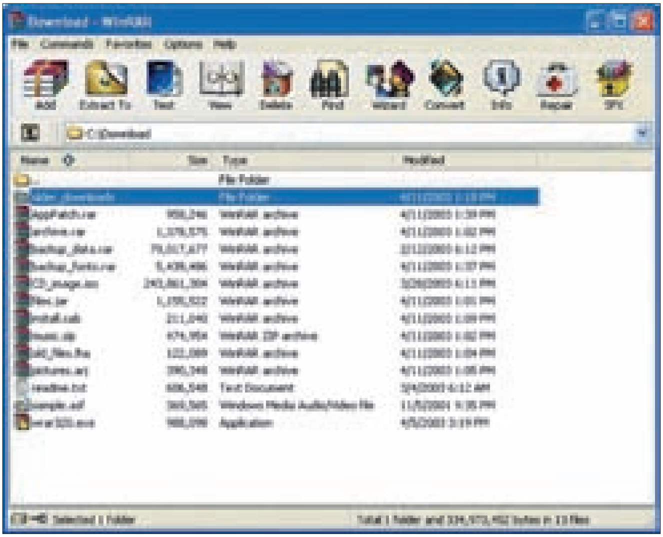
1.4 Backing up important data

What do you do in the event you lose all your data despite taking all precautionary measures. How about if a fire or storm destroys your computer physically? There's also always the risk of data theft. With information becoming more valuable, backing up important data has become vital (according to a Global Backup Survey, 66 per cent of internet users have suffered from serious data loss).

Backup involves making copies of the original data for primarily two situations: Firstly to restore a state following a disaster. The second is to restore a small number of files either accidentally deleted or corrupted – this utilises lesser storage space and keeps efficient track of changes in the data.

There are several means by which one may back up data. Storage media such as external hard disk drives, solid state storage (which includes USB flash drives, thumb drives, etc) and optical discs are usually employed. The last is especially a popular option, especially thanks to the advent of Blu-

Nero 9 has some nice backup options for those who want to backup to optical media



WinRAR will help you save space when backing up, and will also let you protect your backed up data with a password

ray discs that can hold up to 50 GB of data. For writing information to discs, the best software is Nero. It supports all CDs, single- and dual-layer DVDs and now Blu-ray discs. Nero also helpfully indicates how much space the selected files are occupying, especially when it goes over the writable limit. Nero also support multi-session discs for when files are to be added later. Nero Burning Rom 9.4.13.2 is the latest release and the commercial trial can be easily located online.

When dealing with large amounts of data, it becomes important to compress it. This facilitates faster storage and copying speeds, along with fully maximizing any available space. Compression is commonly carried out using WinRAR, wherein the data is stored within archives. Most people would use WinZip but WinRAR supports a wider range of formats, including ZIP files. WinRAR is especially versatile in deciding the compression methods, splitting the info into separate archives of specified sizes (helpfully classified into different categories like DVD5, DVD9, CD, etc) and password protecting archives. It can consistently produce smaller archives than its nearest competition, and supports files/archives of up to 8589 billion GB in size.

Remember the following points: The more important the data, the greater the need for a backup solution.

Chalk out a proper restore strategy, since restoring data through backup can be as taxing as storage. In this case, automated backup and scheduling should be considered. Like regular virus scans, it's easy to forget backing up data or leaving it for another day.

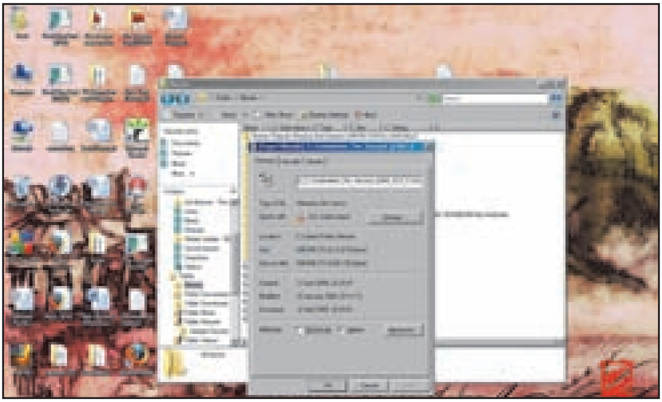
Do not store the backup close to the original data. Fires, rain and electrical surges would likely damage both at the same time. Try storing the backups in an off-site location.

Even if secured properly, backups are not infallible. Verification or monitoring strategies are important for keeping track of the backup's lifeline.

Store backed up archives in open/standard formats. This helps with recovery in the future when the software used to make the backup is obsolete. This allows different software to be used.

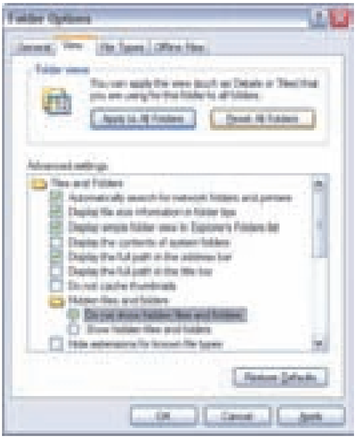
1.5 Hiding files and folders

A hidden file or folder is one that can't normally be seen. This is usually applied to sensitive data such as system files and user preferences to prevent any edits or changes. It also helps when you want to conceal any information from prying eyes. While there are many applications that claim to



Hiding files in Windows

securely hide folders, some cause problems within the operating system. For example, in case of a system crash, will the hidden folders be backed up by the folder hiding application?



You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

Files and Folders
- ☑ Automatically search for network folders and printers
- ☑ Display file size information in folder tips
- ☑ Display simple folder view in Explorer's Folders list
- □ Display the contents of system folders
- ☑ Display the full path in the address bar
- □ Display the full path in the title bar
- □ Do not cache thumbnails

Hidden files and folders
- ● Do not show hidden files and folders
- ○ Show hidden files and folders

- □ Hide extensions for known file types

Making sure hidden files stay hidden

Windows offers a very simple method for hiding folders. Simply right-click on a folder, select Properties, select the Hidden box in Attributes and click OK. The option to hide all subsequent sub-folders and contained files will also be presented. Your folder will now be hidden from public viewing. You can disable the Hidden attribute by deselecting the box. The folder thus reverts back to its visible status.

This is very weak protection since the "protected" folders are still easily viewable. To view any hidden folders (including any system folders), simply go to the Windows Explorer menu. Select `Tools > Folder Options` and go to View. Click on Show Hidden Folders and Files and then Apply To All Folders. This will make all hidden files visible. It should also be noted that Windows allows you to navigate to hidden folders. Simply type the name of the folder in the address bar after the name of the drive and voila.

If they're so easy to uncover, why hide a folder when you can just encrypt it? Simple: You can't want what you can't see. It should never become an either/or choice because you can never be too careful. However, a hidden folder lays in ambiguity. As long as someone doesn't know about it, they won't bother looking for it. However, a password protected folder that is visible screams "important data" and will tempt people to take a crack at it. The best solution is to encrypt and then hide important folders for double security. Simply don't forget the password and you should be fine.

On a side-note, malware often uses the hidden folder options to escape detection. Keep this in mind when running virus scans and having the choice to scan hidden folders as well.

1.6 Recover lost data

When you delete files, they're never permanently deleted. Even if you mistakenly delete a file, it still exists on the hard disk. This is termed as data remanence. The file names are usually only removed from the system directory or shifted to a holding area for safe keeping (even if said area hasn't been specified in advance by the user). One biggest causes of data loss is logical damage. It is primarily caused by power outages that prevent files from being completely written to the storage medium. Problems with hardware like RAID controllers and system crashes usually cause the same but the result is the same. The file system is left in an inconsistent state. This can lead to more problems such as drives reporting negative amounts of free space, system crashes and actual lost data.

Logical damage can be prevented through the use of journaling file systems like NTFS 5.0. It decreases the incidence of logical damage by rolling back to a consistent state. Only the data present in the drive's cache at the time of system failure will be lost. That being said, two common techniques for recovering data from logical damage include:

1. Consistency checking – Scans the logical structure of the disk and makes sure it is consistent with its specifications. A file repair system repair program reads each directory and makes sure these entries exist and point to the correct directories.

2. Data carving – Allows for data with no file system allocation to be extracted by identifying sectors and clusters belonging to the file. Usually searches through raw sectors looking for specific file signatures.

It should be mentioned that data recovery cannot be done on a running system. A boot disk, Live USB, etc. containing a minimal operating system and a set of repair tools is usually required. One of these is Nero BackItUp Image Tool which restores the image created by the application to roll back the system to a consistent state. A good consistency checker is Checkdisk (CHKDSK, for short). It runs on DOS, OS/2 and

Windows OS systems, displaying file system integrity status of disk drives. It can fix logical file system errors and can also check the disk surface for physical errors or bad sectors. CHKDSK can be run from the Windows Shell, the Windows Command Prompt or the Windows Recovery Console.

Some general tips for recovering data: Don't delete files instantly. Move them to a temporary location such as the recycle bin before deciding whether you need them or not.

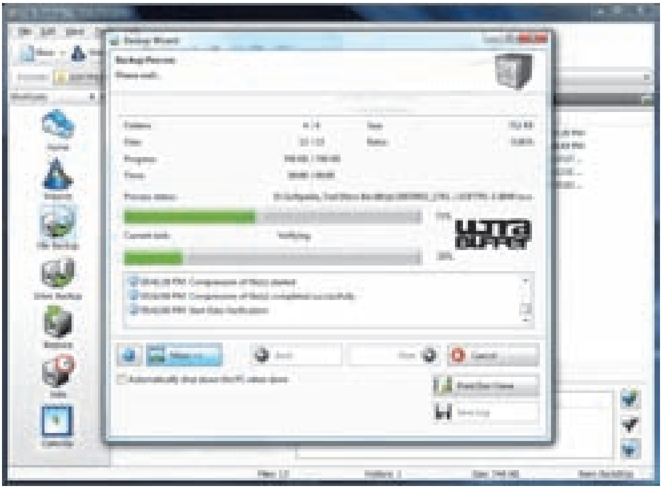
Mark important files as read-only. The OS will then warn you if you try to delete the file. Under systems that allow file system permissions, users can often only delete their own files. This prevents the erasure of critical system files or other's work.

1.7 Securely delete data

The reasons for deleting files are many: Freeing disk space, removing unnecessary or unneeded data, even making sensitive data unavailable to others. However, securely deleting data involves more than simply emptying the Recycle Bin. Basic file deletion methods only remove he direct pointers to data disk centres. A residual form of the data, called data remanence, still persists. Thus, any one with data recovery tools can still unearth the data once more. Physical destruction may seem like the only way but thankfully, there exist many data erasure methods that remove information permanently while still keeping the disk operable.

Software-based overwriting is one such method. It writes patterns of meaningless data onto each of a hard drive's sectors. It differs from pure data erasure in that some data will still be intact and at risk of data breach or information theft. Nonetheless, data erasure employs multiple overwrites according to different overwriting standards. There are usually three types of data erasure that differ depending on the number of overwrites:

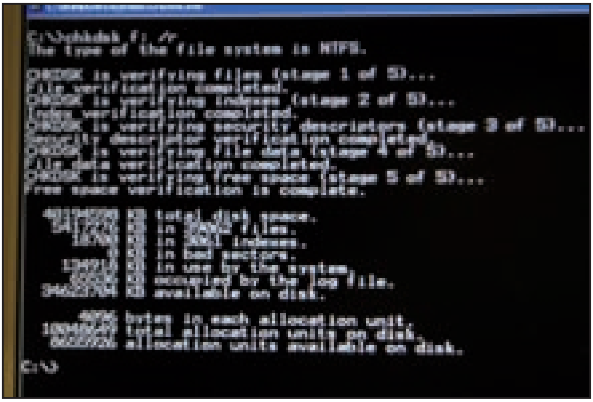
1. Fast erasure – Consists of one round of data deletion and the filling of space with random data.
2. Forced erasure – A US Department of Defense standard of file erasure. Unlike quick erase, data is overwritten with useless info 3 to 7 rounds in a row. Also referred to as the DoD 5220.22M Standard.



Using Nero BackItUp to back up files

3. Ultimate erasure – The erased file goes through 35 rounds of overwriting, first with a lead-in four random write patterns, 5-31 patterns executed in random order and a lead-out of four more random patterns. This method is also referred to Gutmann Algorithm.

The data overwriting the existing data consists of little



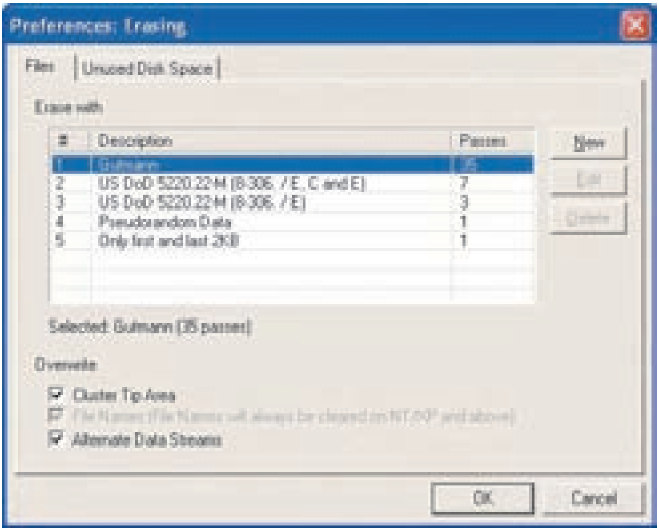
```
C:\>chkdsk f: /r
The type of the file system is NTFS.

CHKDSK is verifying files (stage 1 of 5)...
File verification completed.
CHKDSK is verifying indexes (stage 2 of 5)...
Index verification completed.
CHKDSK is verifying security descriptors (stage 3 of 5)...
Security descriptor verification completed.
CHKDSK is verifying file data (stage 4 of 5)...
File data verification completed.
CHKDSK is verifying free space (stage 5 of 5)...
Free space verification is complete.

  [illegible] KB total disk space.
  [illegible] KB in [illegible] files.
  [illegible] KB in [illegible] indexes.
  [illegible] KB in bad sectors.
  [illegible] KB in use by the system.
  [illegible] KB occupied by the log file.
  [illegible] KB available on disk.

        4096 bytes in each allocation unit.
  [illegible] total allocation units on disk.
  [illegible] allocation units available on disk.

C:\>
```

Using chkdisk

more than random numbers or a series of zeroes and ones bit patterns.

Freeraser: Free Shredder is a Windows file shredding utility that wipes files in all three of the above methods and is good for basic use. It even places a fancy recycle bin icon that prompts a warning message any time you drag any data to it. Eraser Secure Data Removal Tool goes even further by can also erase space allocated to the file by the OS (called file slack space), Windows virtual memory swap files, unused space on a hard disk or an entire hard disk and also erasing filenames from the directories. It can wipe any amount of data specified and even supports the three above erasure methods. It's also open source and works perfectly with Windows.

Let's say you want to completely wipe your hard disk, when giving away your computer to someone for example. No other software is best suited for bulk emergency destruction than Darik's Boot and Nuke, referred to as DBAN for short. It comes in the form of bootable CDROM image and once loaded proceeds to completely destroy data in every partition and hard disk.



Erase with

#	Description	Passes
1	Gutmann	35
2	US DoD 5220.22-M (8-306. / E, C and E)	7
3	US DoD 5220.22-M (8-306. / E)	3
4	Pseudorandom Data	1
5	Only first and last 2KB	1

Selected: Gutmann (35 passes)

Overwrite

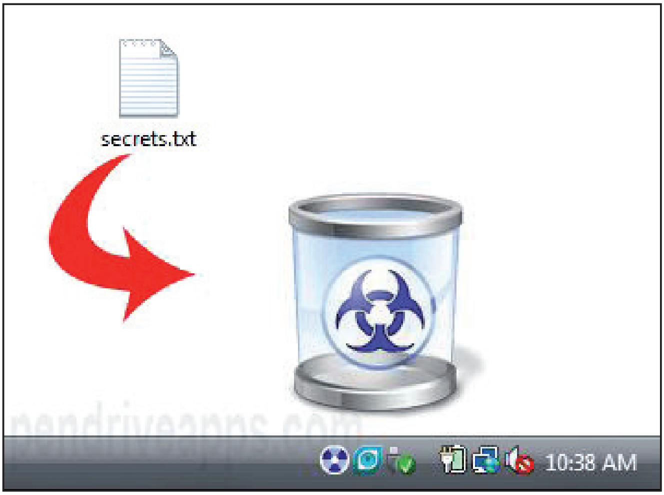
☑ Cluster Tip Area
☑ File Names (File Names will always be cleared on NT/XP and above)
☑ Alternate Data Streams

Erasing data securely

A PC can have more than one user. For more than one user, especially with children, it's always good to keep more than one user profile. However, it's important to specify which files a user can be allowed to access and manipulate. Windows usually keeps most important system files hidden but they can still be modified. Hence, controlling accessibility becomes a major part of computer security especially when your computer is cracked.

To modulate accessibility, first go to the Control Panel >User Accounts and make sure more than one account is active (preferably one with administrator access and one "guest" account). Then right-click on the My Computer icon, select Properties and go to the Advanced tab. Options for Performance, User Profiles and Start-up & Recovery will be available. Select User Profiles and depending on your accounts set, you can specify which drives different users will access. You can also set up groups to decide who can access which drives and documents.

Creating a Limited access account, with no access to the important system files has its advantage on open networks and wi-fi connections. Sharing networks over a wi-fi easily allows another user to access one's files and hard drives for malicious purposes. Viruses and spyware present on the main server system will also infect other computers in the



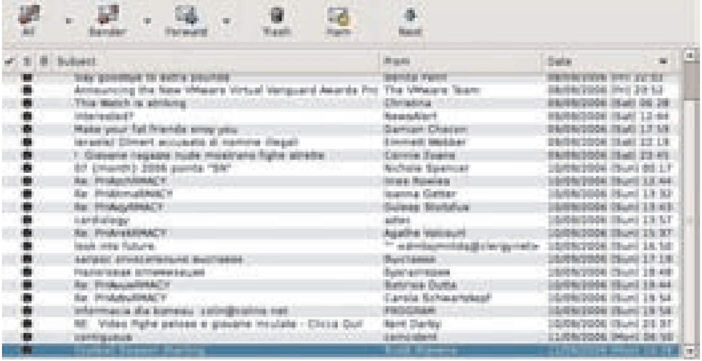
network. You should have an anti-virus, anti-spyware and firewall installed on the system. But locking out access to the vital system files will eliminate the extra 1% of intrusions that make it through.

2.1 Spam filters

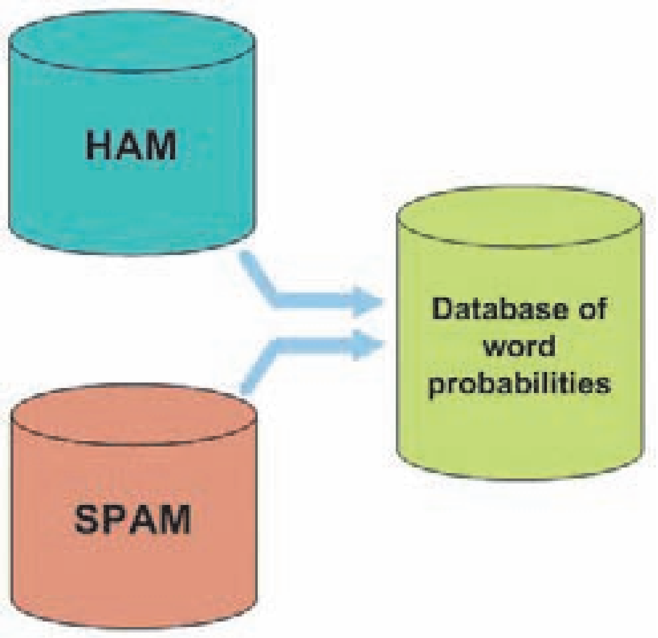
Spam is a growing problem for email users, and many solutions have been proposed, from a postage fee for email to Turing tests to simply not accepting email from people you don't know. Spam filtering is one way to reduce the impact of the problem on the individual user (though it does nothing to reduce the effect of the network traffic generated by spam). In its simplest form, a spam filter is a mechanism for classifying a message as either spam or not spam.

There are many techniques for classifying a message. It can be examined for "spam-markers" such as common spam subjects, known spammer addresses, known mail forwarding machines, or simply common spam phrases. The header and/or the body can be examined for these markers. Another method is to classify all messages not from known addresses as spam. Another is to compare with messages that others have received, and find common spam messages.

A popular spam filter is SpamAssassin. It's an extensible email filter that is used to identify spam. Once identified, you can optionally tag it as spam for later filtering. It also provides a command line tool to perform filtering, a client-server system for larger volumes and Mail::SpamAssassin, a set of Perl modules allowing SpamAssassin to be used in a wide variety of email system. It's also become much easier to blacklist and whitelist messages than before. SpamAssassin also comes equipped with Bayesian filters that can identify spam and non-spam (called "ham") based on certain keywords or "tokens" that appear



SpamAssassin is effective in identifying email spam



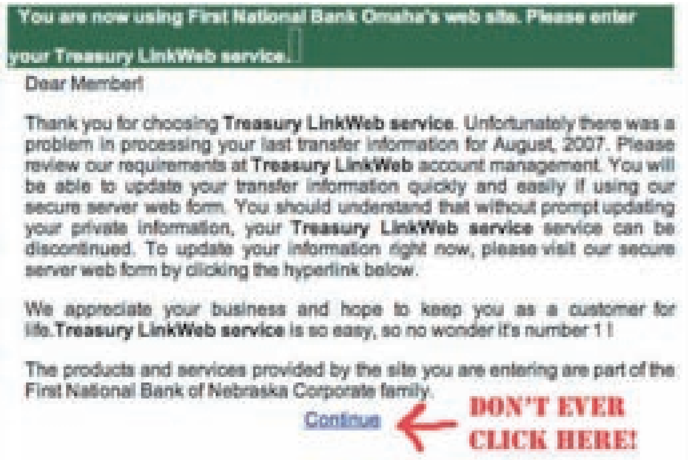
Bayesian filters get more effective with each spam mail identified

frequently in spam messages. The more spam (and ham) you filter, the better it gets at detecting spam.

If you can't use a filter, what then? The most common solution is to have multiple email addresses. One approach is to select one to be your "private" guarded email address - much like an unlisted phone number - that you never use in situations where the email address would be harvested for spam mailing lists. The other approach is to generate "throw-away" email addresses that you use only for a limited time (say when registering a product), and can safely ignore thereafter. And of course both approaches can be used at the same time.

2.2 Identifying hoaxes

A hoax can best be defined as a deliberate attempt to trick people into believing or something to be real. Internet hoaxes are no different. If you've received any mails claiming that you've



You are now using First National Bank Omaha's web site. Please enter your Treasury LinkWeb service.

Dear Member!

Thank you for choosing **Treasury LinkWeb service**. Unfortunately there was a problem in processing your last transfer information for August, 2007. Please review our requirements at **Treasury LinkWeb** account management. You will be able to update your transfer information quickly and easily if using our secure server web form. You should understand that without prompt updating your private information, your **Treasury LinkWeb service** service can be discontinued. To update your information right now, please visit our secure server web form by clicking the hyperlink below.

We appreciate your business and hope to keep you as a customer for life.**Treasury LinkWeb service** is so easy, so no wonder it's number 1 !

The products and services provided by the site you are entering are part of the First National Bank of Nebraska Corporate family.

Continue

DON'T EVER CLICK HERE!

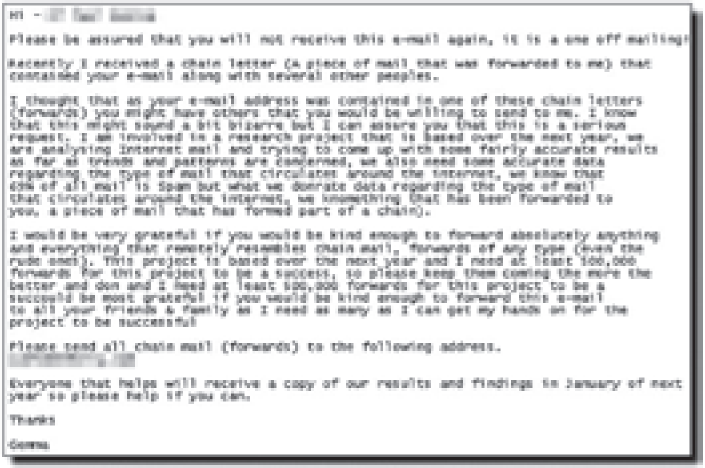
Think twice before clicking on inviting links

won millions in some random foreign lottery (with the key to receiving these millions being to pay some money up front), you'll know what we mean. The perpetrators behind these messages want nothing more than for you to mail them your credit card/bank account numbers.

The best way to spot hoaxes is a good dose of common sense. As the saying goes, "If it sounds too good to be true, it usually is". The Internet Crime Complaint Center, Federal Trade Commission and Better Business Bureau all recommend the following tips for protecting your personal info.

- Do not respond to the scam email, click on links, or open attachments, which could leave your computer at risk for viruses.
- If the email appears to have come from a company, check their web site to see if they've addressed any scams using their name, and contact the Better Business Bureau to find out if there have been any complaints about such a scam.

In case you've responded to what you believe was a scam, then make sure to contact your bank immediately and ask what steps you should take to protect your money. You should also review your free credit report to monitor your active accounts, mortgages, and other financial information. Always treat email



Hi - [redacted]

Please be assured that you will not receive this e-mail again, it is a one off mailing!

Recently I received a chain letter (A piece of mail that was forwarded to me) that contained your e-mail along with several other peoples.

I thought that as your e-mail address was contained in one of these chain letters (forwards) you might have others that you would be willing to send to me. I know that this might sound a bit bizarre but I can assure you that this is a serious request. I am involved in a research project that is based over the next year, we are analyzing Internet mail and trying to come up with some fairly accurate results as far as trends and patterns are concerned, we also need some accurate data regarding the type of mail that circulates around the internet, we know that 40% of all mail is Spam but what we dont have data regarding the type of mail that circulates around the internet, we (something that has been forwarded to you, a piece of mail that has formed part of a chain).

I would be very grateful if you would be kind enough to forward absolutely anything and everything that remotely resembles chain mail, forwards of any type (even the rude ones!). This project is based over the next year and I need at least 500,000 forwards for this project to be a success, so please keep them coming the more the better and don and I need at least 500,000 forwards for this project to be a successI would be most grateful if you would be kind enough to forward this e-mail to all your friends & family as I need as many as I can get my hands on for the project to be successful!

Please send all chain mail (forwards) to the following address.
[redacted]

Everyone that helps will receive a copy of our results and findings in January of next year so please help if you can.

Thanks

Gemma

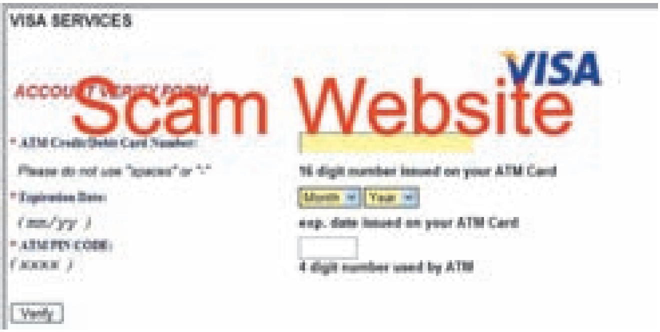
Always look out for the typical style in scam emails

solicitations with skepticism, since there's no way to avoid receiving these mails. If you didn't remember signing up for a service or contest, then you probably didn't. Reputable financial institutions never prompt you for account information via email, but if you're unsure about whether you need to provide extra info to a company you deal with, always contact them directly.

Another kind of hoax is the infamous chain letter. These try to persuade the recipient to forward the letter to as many people as possible by using emotional stories or get-rich-quick schemes. There's also the threat of physical violence or bad luck if one attempts to break the chain. It can often become difficult to tell the difference between chain letters and real correspondence, since it's not uncommon for people to treat it like a game. Chain letters are widely popular on sites such as Orkut and Youtube, with some comments prompting the user to copy and paste a link to get secret information. Naturally, you should never follow such links nor open any attachments that come with chain letters since they can contain trojans.

2.3 Identifying scams

Hoaxes attempt to fool people into dropping some cash. Scams can be a lot more dangerous, since they attempt to obtain all



VISA SERVICES

ACCOUNT VERIFY FORM

* ATM Credit/Debit Card Number:
Please do not use "spaces" or "-"
16 digit number issued on your ATM Card

* Expiration Date:
(mm/yy)
exp. date issued on your ATM Card

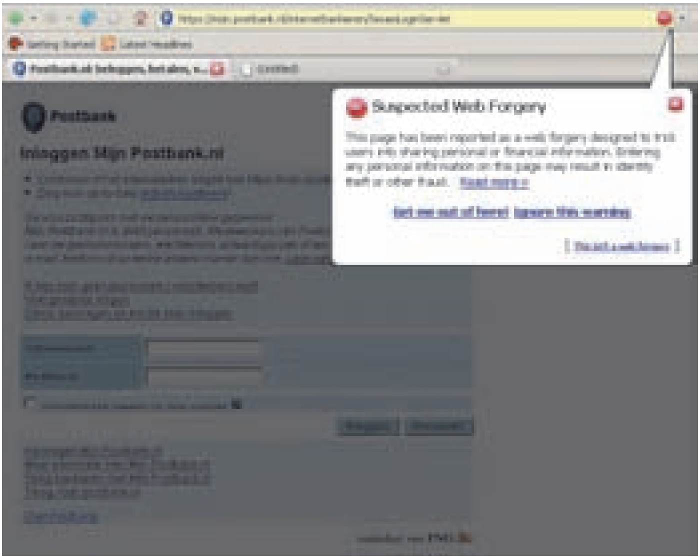
* ATM PIN CODE:
(xxxx)
4 digit number used by ATM

Be cautious, especially during online financial transactions

types of sensitive info. Be it passwords, usernames or credit card details, scams can be very hard to identify at times. They can be in the form of messages from popular social web site, auction sites, IT admins and even job seeking sites. It's typically carried out by email and instant messaging, though scams are also possible through phone calls. Users are prompted to enter info that often looks and works exactly like the legitimate one, even under severe scrutiny via server authentication.

Since scams go the extra mile to get info from their users, they require more than just a little common sense to deal with.

- Even if the mails look like they're from familiar people, they could be from scammers and contain programs that will steal your personal information.
- Watch out for "phishy" emails. The most common form of scamming are emails pretending to be from a legitimate retailer, bank, organization, or government agency. The sender asks to "confirm" your personal information for some made-up reason: your account is about to be closed, an order for something has been placed in your name, or your information has been lost because of a computer problem.
- Don't click on links within emails that ask for your personal information. Fraudsters use these links to lure people to phony web sites that looks just like the real sites of the company, organization, or agency they're impersonating. Always verify the web site from the company or agency, call it directly or go to its web site via



This page has been reported as a web forgery designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud.

Most browsers give out a warning when suspicious activities are detected

search engine.

- A scammer can direct you to a real company's web site, but then an unauthorised pop-up screen created by the scammer will appear, with blanks in which to provide your personal information. Never provide information in these. Installing pop-up blocking software helps prevent this.
- A spam filter can help reduce the number of scam mails you get. Anti-virus software as explained earlier can scan for malicious files and report any suspicious activity taking place on your PC. Firewalls will prevent unauthorised communications from entering your computer. Look for programs that offer automatic updates and take advantage of free patches that manufacturers offer to fix newly discovered problems.

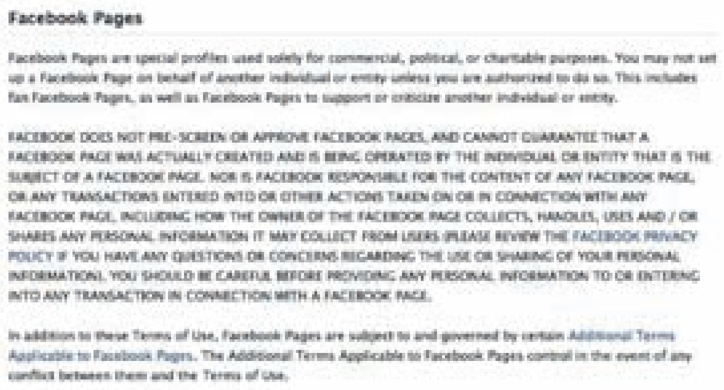
Most browsers these days maintain a list of known scam sites and check web sites against the list. Mozilla Firefox 2 onwards uses Google's anti-phishing software, which has found be more effective than Internet Explorer 7 onwards in detecting fraudulent sites.

2.4 Protecting your profile on social networking sites

Social networking sites are the hottest places to meet people online nowadays. Interest groups, blogs, chatting, hobbies, friends, business networking – these sites mimic all the aspects of real life socialising but online. Just like real life, however, you're open to attacks and theft of information online. When setting up a profile on a social networking site like Facebook or Myspace, it's essential to determine what info you wish to post. Your name, age, gender, zip code and email address are usually required to create an account. The info that should never be shared on your profile include: Address, phone number, social security number and credit card number.

It's not just about the info you share but who you want to share it with. When you first join a social networking site, the default setting is to allow anyone to see your profile and updates. Sites such as Facebook go even further: Your activities will not only be shared with various friends and groups, but also across every single network you've ever traversed. You can disable these settings in the account settings and unchecking "Allow anyone to see my public search listing" along with restricting your email IDs, IM names and other details to people on your friends list.

It's vital to understand the privacy policy of some of



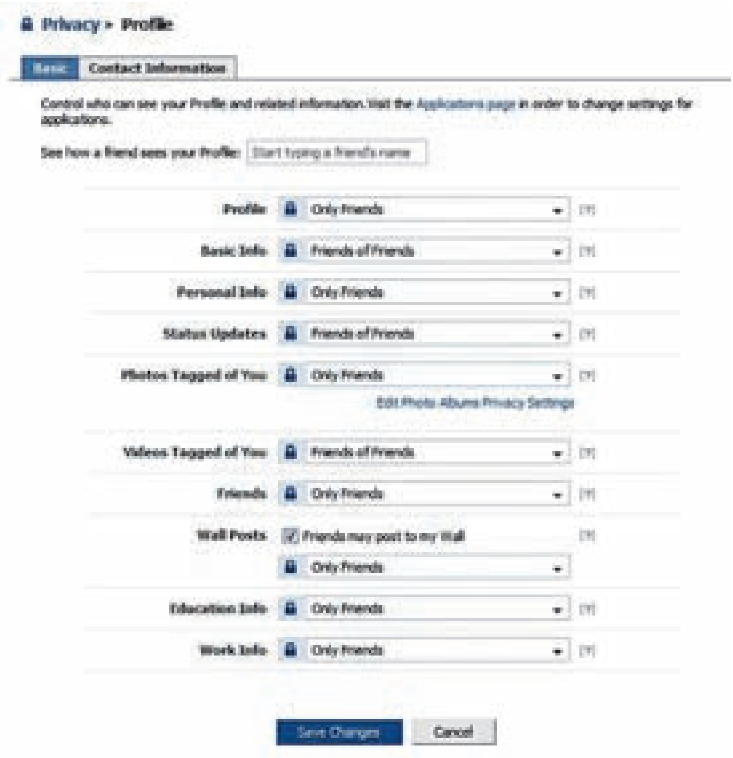
Facebook Pages

Facebook Pages are special profiles used solely for commercial, political, or charitable purposes. You may not set up a Facebook Page on behalf of another individual or entity unless you are authorized to do so. This includes fan Facebook Pages, as well as Facebook Pages to support or criticize another individual or entity.

FACEBOOK DOES NOT PRE-SCREEN OR APPROVE FACEBOOK PAGES, AND CANNOT GUARANTEE THAT A FACEBOOK PAGE WAS ACTUALLY CREATED AND IS BEING OPERATED BY THE INDIVIDUAL OR ENTITY THAT IS THE SUBJECT OF A FACEBOOK PAGE. NOR IS FACEBOOK RESPONSIBLE FOR THE CONTENT OF ANY FACEBOOK PAGE, OR ANY TRANSACTIONS ENTERED INTO OR OTHER ACTIONS TAKEN ON OR IN CONNECTION WITH ANY FACEBOOK PAGE, INCLUDING HOW THE OWNER OF THE FACEBOOK PAGE COLLECTS, HANDLES, USES AND / OR SHARES ANY PERSONAL INFORMATION IT MAY COLLECT FROM USERS (PLEASE REVIEW THE FACEBOOK PRIVACY POLICY IF YOU HAVE ANY QUESTIONS OR CONCERNS REGARDING THE USE OR SHARING OF YOUR PERSONAL INFORMATION). YOU SHOULD BE CAREFUL BEFORE PROVIDING ANY PERSONAL INFORMATION TO OR ENTERING INTO ANY TRANSACTION IN CONNECTION WITH A FACEBOOK PAGE.

In addition to these Terms of Use, Facebook Pages are subject to and governed by certain Additional Terms Applicable to Facebook Pages. The Additional Terms Applicable to Facebook Pages control in the event of any conflict between them and the Terms of Use.

Carefully read the privacy policy of the web sites that gather your personal information



Privacy ▸ Profile

Basic | Contact Information

Control who can see your Profile and related information. Visit the Applications page in order to change settings for applications.

See how a friend sees your Profile: Start typing a friend's name

Profile: Only Friends [?]

Basic Info: Friends of Friends [?]

Personal Info: Only Friends [?]

Status Updates: Friends of Friends [?]

Photos Tagged of You: Only Friends [?]

Edit Photo Albums Privacy Settings

Videos Tagged of You: Friends of Friends [?]

Friends: Only Friends [?]

Wall Posts: ☑ Friends may post to my Wall [?]
Only Friends

Education Info: Only Friends [?]

Work Info: Only Friends [?]

When filling your profile, make sure you don't let anonymous people have access to your personal information

these social networking sites. Is the policy easy to read and understand? Will they share or sell your information? How recently was it updated? Sites like LinkedIn state plainly that will never sell your info. Facebook and Myspace do not state they won't sell your info so it's safe to assume they're reserving the right to do so.

By default, everyone can find your profile listing in a public search. This includes Facebook and Myspace, along with the potential to find people across MSN, Google and Yahoo. Make sure you go through the Privacy Settings of your account to ascertain which information you'd like to display publicly. Alternatively, you can set your profile to "No Networks" in Facebook which will disable most sharing settings. Selecting the "My Friends Only" box in Myspace will lock out strangers from viewing your profile.

A trick used to gain information involves some one creating a new account with your friend's name and a few general details. Then they send a friend request to you, stating they've created a new account (for some reason or another). In this case, confirm with your friend personally or over his old account whether the new account is real or not.

2.5 Using secure passwords

Passwords are the keys to access personal information stored in your computer. This means they are the one barrier between your data being safe and sound to having your entire system compromised.

The strongest passwords are those that are the longest. Most passwords should at least be 8 characters in length but those with 14 or more characters are the best. Combine letters, numbers and symbols culled from the entire keyboard. Your password will be much stronger if you choose from all symbols on the keyboard, including punctuation marks not on the upper row of the keyboard and even symbols unique to your own language. Substitute letters with similar looking numbers (for example, "A" with "4") and also mix uppercase and lowercase letters. Throw some misspellings in there as well.

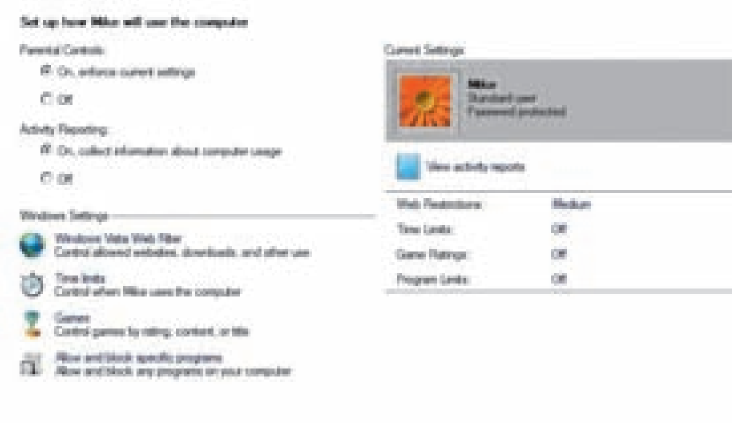
The greater variety of characters in your password, the harder it is to guess. If you cannot create a password that contains symbols, you need to make it considerably longer to get the same degree of protection. An ideal password is one that combines both length and different characters. Finally, use words and phrases that are easy for you to remember but difficult for others to guess.

The various don'ts to follow when making a strong password are:

- Avoid sequences or repeated characters. "12345678," "222222," "abcdefg," or adjacent letters on your keyboard do not help make secure passwords.
- Avoid using only look-alike substitutions of numbers or symbols. Criminals and other malicious users who know enough to try and crack your password will not be fooled by common look-alike replacements, such as to

replace an 'i' with a '1' or an 'a' with '@' as in "M1cr0$0ft" or "P@ssw0rd". But these substitutions can be effective when combined with other measures, such as length, misspellings, or variations in case, to improve the strength of your password.

- Avoid your login name. Any part of your name, birthday, social security number, or similar information for your loved ones constitutes a bad password choice. This is one of the first things criminals will try.
- Avoid dictionary words in any language. Criminals use sophisticated tools that can rapidly guess passwords that are based on words in multiple dictionaries, including words spelled backwards, common misspellings, and substitutions. This includes all sorts of profanity and any word you would not say in front of your children.
- Use more than one password everywhere. If any one of the computers or online systems using this password is compromised, all of your other information protected by that password should be considered compromised as well. It is critical to use different passwords for different systems.
- Avoid using online storage. If malicious users find these passwords stored online or on a networked computer, they have access to all your information.



Set up how Mike will use the computer

Parental Controls:

● On, enforce current settings

○ Off

Activity Reporting:

● On, collect information about computer usage

○ Off

Windows Settings

Windows Vista Web Filter
Control allowed websites, downloads, and other use

Time limits
Control when Mike uses the computer

Games
Control games by rating, content, or title

Allow and block specific programs
Allow and block any programs on your computer

Current Settings:

Mike
Standard user
Password protected

View activity reports

Web Restrictions	Medium
Time Limits	Off
Game Ratings	Off
Program Limits	Off

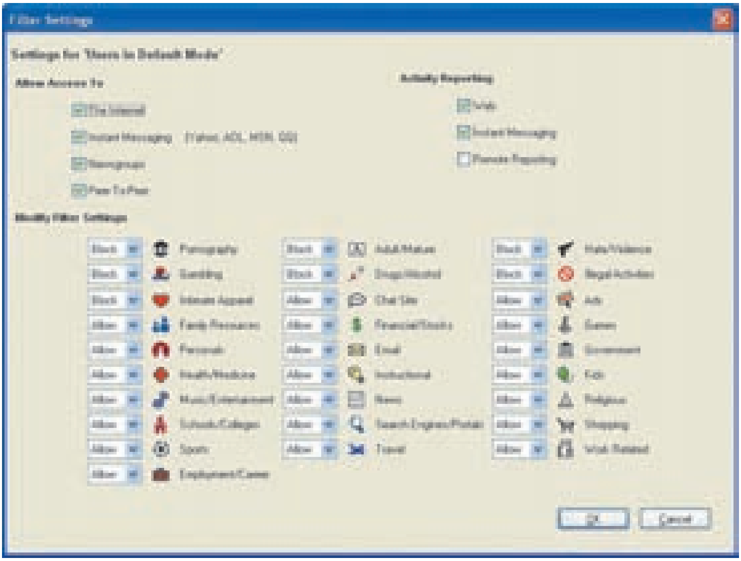
Windows has some effective parental control options

- Change your password every 30-60 days and avoid using any old password.

You can also generate any random password of your liking very easily through PC Tools Secure Password Generator at:
http://www.pctools.com/guides/password/

2.6 Restricting children to safe areas

Children working off the same computer or connecting to the internet the first time, especially in this age of net crimes, are always at risk. However, explicit content and malware also pose a significant threat for a child who wouldn't be able to deal with them. There are several parental controls embedded within Windows. You have the option of turning them on or off, as well as collecting information about computer usage by enabling Activity Reporting. First go to the Control Panel and click on `User Accounts>Parental Controls`. You can apply Parental Controls on pre-existing, non-administrator account or create a new one for the purpose. The different control options



Filter Settings

Settings for 'Users in Default Mode'

Allow Access To

☑ The Internet
☑ Instant Messaging (Yahoo, AOL, MSN, ICQ)
☑ Newsgroups
☑ Peer To Peer

Activity Reporting

☑ Web
☑ Instant Messaging
□ Remote Reporting

Modify Filter Settings

Block Pornography
Block Gambling
Block Intimate Apparel
Allow Family Resources
Allow Personals
Allow Health/Medicine
Allow Music/Entertainment
Allow Schools/Colleges
Allow Sports
Allow Employment/Career

Block Adult/Mature
Block Drugs/Alcohol
Allow Chat Site
Allow Financial/Stocks
Allow Email
Allow Instructional
Allow News
Allow Search Engines/Portals
Allow Travel

Block Hate/Violence
Block Illegal Activities
Allow Ads
Allow Games
Allow Government
Allow Kids
Allow Religious
Allow Shopping
Allow Work Related

With Net Nanny, you can keep a tab on what kids can see online

include the following:

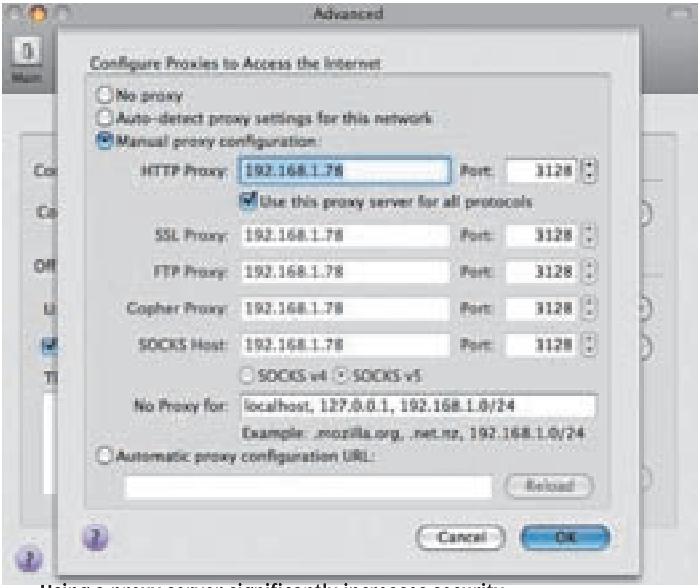
- Web filter – Contains an Allow and Block list which you can edit. You can also choose to block some websites or allow all websites for the user to visit. Also allows you to modify the restriction level of the web based on key categories and block file downloads.
- Time Limits – You can set the time for which a user is able to use the computer. You can select different hour slots within the week and easily mark out which are to be blocked with a single click.
- Game Controls – Allows you to set the ratings for the games the user is allowed to play. You can also block or allow specific games on the computer.
- Application Restrictions – Let's you determine if the user can access all programs or only the ones you allow.

You can also third party web content filter software for maximum protection. A very effective one is Net Nanny. It can block illegal file sharing and even social networking sites. It also allows for remote management and monitoring of instant messaging programs such as AIM. The latter is especially important when taken into account with the number of malicious crimes perpetrated beginning from a simple chat conversation.

It's important to advise your kids on safe surfing. Advise them on not speaking to strangers and explain how it's very easy for someone to be misled on the internet. Tell them which sites they're allowed to visit any why. Warn them about freely exploring on their own, as well as not to download any applications from the internet that come from questionable sites or. They should also inform you whether they receive any emails from people they don't know. Explain the risks of viruses as well as the need to be careful even with attachments from people they know. Finally, if kids receive an email they don't like from someone they don't know, tell them to inform you immediately and not to reply themselves.

2.7 Using internet proxies

As stated earlier, internet proxies act as go-betweens for requests from clients seeking resources from other serves. This is meant for the purpose of either keeping the machines anonymous or



Advanced

Configure Proxies to Access the Internet

○ No proxy
○ Auto-detect proxy settings for this network
● Manual proxy configuration:

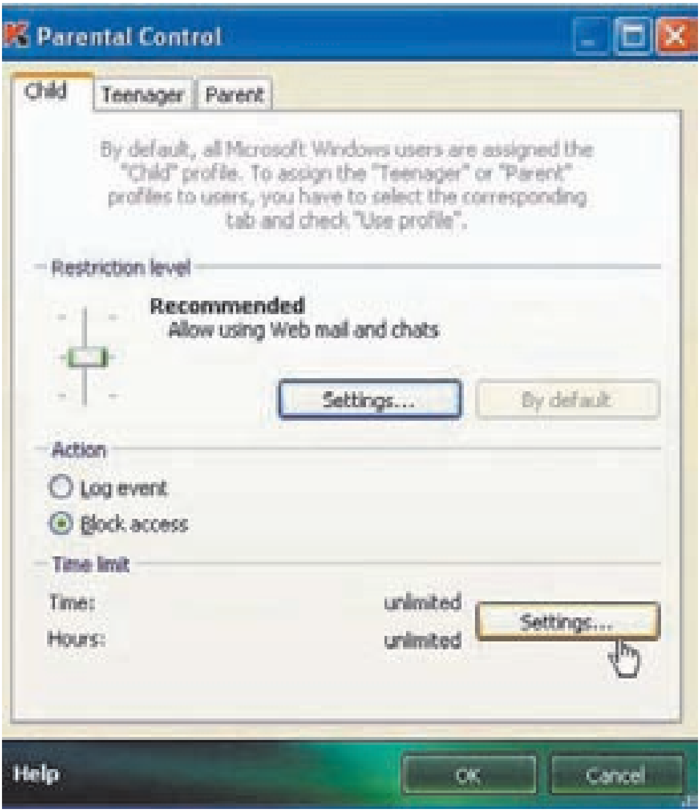
HTTP Proxy: 192.168.1.78 Port: 3128
☑ Use this proxy server for all protocols
SSL Proxy: 192.168.1.78 Port: 3128
FTP Proxy: 192.168.1.78 Port: 3128
Gopher Proxy: 192.168.1.78 Port: 3128
SOCKS Host: 192.168.1.78 Port: 3128
○ SOCKS v4 ● SOCKS v5
No Proxy for: localhost, 127.0.0.1, 192.168.1.0/24
Example: .mozilla.org, .net.nz, 192.168.1.0/24
○ Automatic proxy configuration URL:

Using a proxy server significantly increases security

speeding up access to a resource via caching. The two main proxies we'll talk about are web proxies and content filtering proxies.

Web proxies are those focusing on www traffic. The most common use for a web proxy is in web caching. Caching keeps local copies of frequently requested resources allowing one to significantly reduce their upstream bandwidth cost and usage while increasing performance. Some web proxies also provide a means to deny access to certain URLs in a blacklist, thus providing for some form of content filtering.

One of the more well-known freeware web proxies is Squid. It functions as a proxy server and a web cache daemon. It serves a variety of uses from speeding up a web server to caching repeated requests. It also caches web, DNS, and other computer network lookups for people sharing network resources. Squid also aids in filtering traffic thus aiding in security. It also has some features that can help anonymize connections such as disabling or changing specific header fields in a client's HTTP



By default, all Microsoft Windows users are assigned the "Child" profile. To assign the "Teenager" or "Parent" profiles to users, you have to select the corresponding tab and check "Use profile".

Restriction level

Recommended
Allow using Web mail and chats

Action

○ Log event
● Block access

Time limit

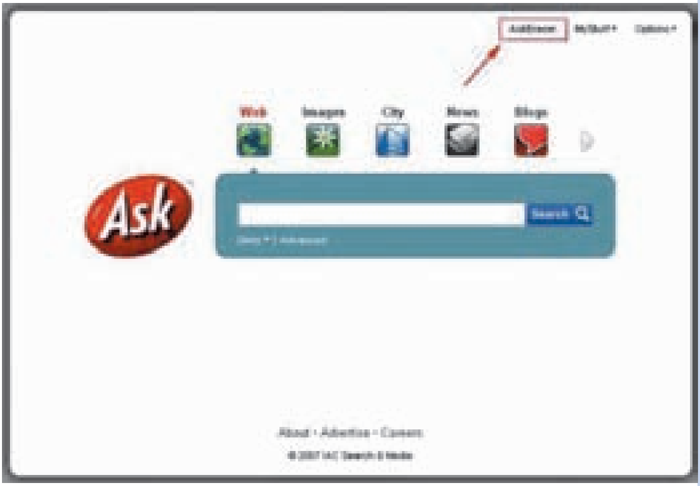
Time: unlimited
Hours: unlimited

Web filters keep offensive content from innocent kids

requests. Whether they are set and what they are set to do is up to the person who controls the computer running Squid.

Squid can also function as a reverse proxy – that is, serving an unlimited number of clients for a limited number of webservers. This results in less traffic to the source server, meaning less CPU and memory usage, and less need for bandwidth. All without any action by the clients. Squid works on a variety of platforms, including Windows, Linux, Mac OS X, etc.

Content filtering proxies, also known as censorware



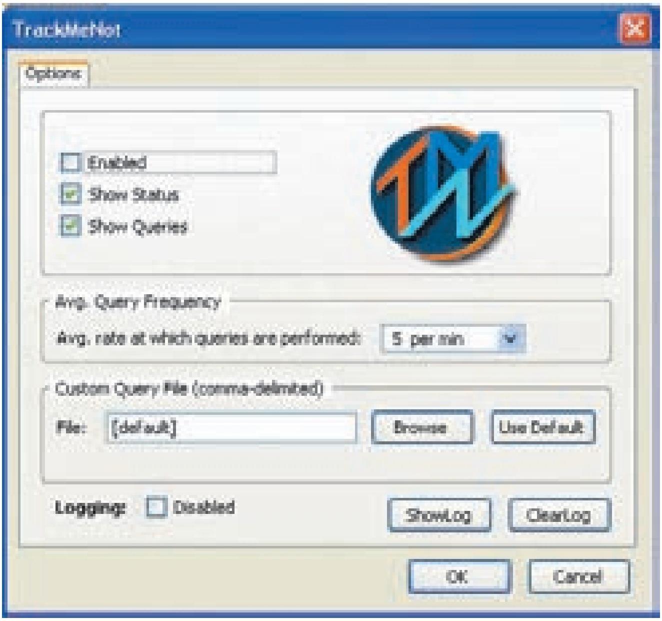
Ask Eraser deletes all your search queries to protect your privacy

or web filtering software, is a term for software designed and optimised for controlling what content is permitted to a reader, especially when used to restrict material delivered over the web. Content-control software determines what content will be available on a particular machine or network. The motive is often to prevent persons from viewing content which may be considered objectionable.

2.8 Avoid leaving a search trail

A search query is a term a user enters into a search engine to satisfy information needs. When a user records the path of the queries and the information they lead to, it is referred to as a search trail. The trails themselves are searchable, allowing users to save time when searching by examining pages found by other users. The intention is also to allow easier searching of the web. An application that lets users record search trails is Trexy, which installs itself as a toolbar and records the user's activity on search sites it is aware of.

However, some major sites such as Google, AOL,



☐ Enabled
☑ Show Status
☑ Show Queries

Avg. Query Frequency
Avg. rate at which queries are performed: 5 per min

Custom Query File (comma-delimited)
File: [default]

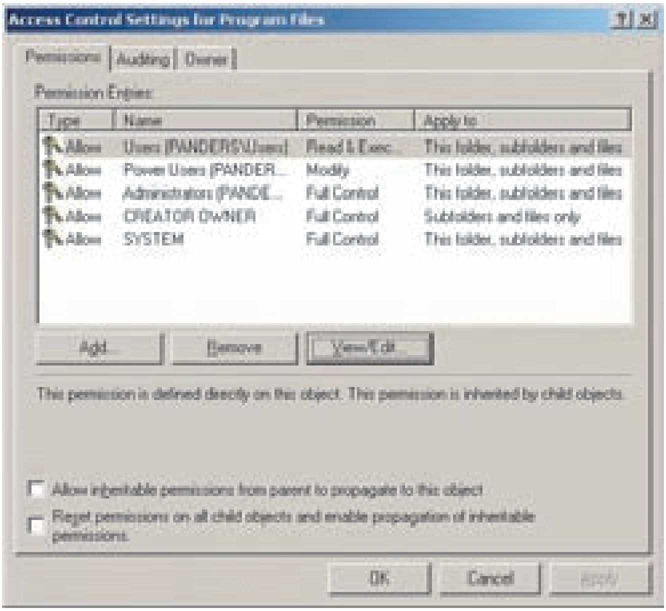
Logging: ☐ Disabled

TrackMeNot makes your search behaviour difficult to analyse

Yahoo and MSN are all collecting data from users. All of this search engines are monitoring and storing your searches along with other such data as your behaviour while online. This information may in some cases, not only been seen by those involved with your favourite search engine but also in many cases, third parties. Some sites such as Ask.com allow users to delete data on search queries to bolster personal privacy. Called AskEraser, it deletes all subsequent search queries and related information linked to a user's cookies or identifying information from computers. It's featured on the site's home page and all search results pages, with a clear choice to signal whether the feature should be "On" or "Off" during a user's search requests.

Another option is to hide your search in a cloud of "ghost queries". A Firefox add-on called TrackMeNot does just that. On installing, it will show up in your status bar with certain search queries. These will be sent to search engines faking them out as to where you are really going or what you are searching for while online. You can disable the display if you so desire. The same options are also available from the Tools menu of the browser. You can also set the Search Engines that TrackMeNot queries, queries to be set, query frequency and the logging options for the performed queries. Keep in mind that if third parties are using other means to identify you, such as through IP addresses and information from your ISP, TrackMeNot will be of little use. However, in terms of identifying you through searches alone, TrackMeNot potentially makes this a lot more difficult for third parties.

2.9 Restrict access to content hosted on a personal space



Access Control Settings for Program Files

Permission Entries:

Type	Name	Permission	Apply to
Allow	Users (PANDERS\Users)	Read & Exec...	This folder, subfolders and files
Allow	Power Users (PANDER...	Modify	This folder, subfolders and files
Allow	Administrators (PANDE...	Full Control	This folder, subfolders and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	SYSTEM	Full Control	This folder, subfolders and files

This permission is defined directly on this object. This permission is inherited by child objects.

□ Allow inheritable permissions from parent to propagate to this object

□ Reset permissions on all child objects and enable propagation of inheritable permissions.

With NTFS, you can now modify access rights depending on the criticality

Windows uses two types of file systems: FAT and NTFS. In computing, a file system is a method for storing data and making it easy to find and access. Regarding the performance of FAT and NTFS, FAT performs better on smaller volumes, but NTFS out-performs FAT on larger volumes, beginning around 500MB.

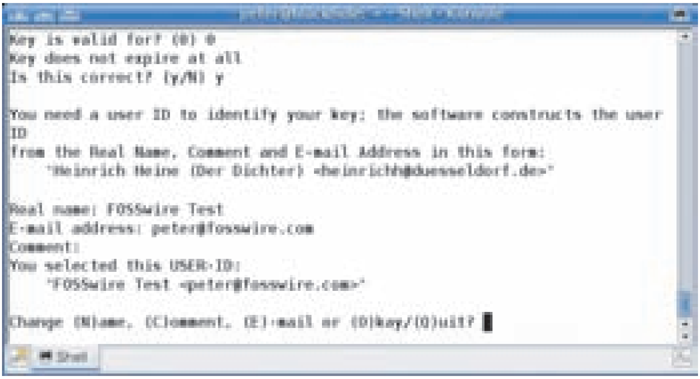
NTFS, short for New Technology File System, is the most secure and robust file system for Windows. It provides security by supporting access control and ownership privileges, meaning you can set permission for groups or individual users to access certain files. This can thus be used to restrict access to content hosted on personal space.

NTFS has several key features. It supports compression of individual files and folders which can be read and written to while they are compressed. It's a recoverable file system, meaning it has the ability to undo or redo operations. It also supports Macintosh files. The NTFS 5.0 file system can also automatically encrypt and decrypt file data as it is read and written to the disk. It will put restrictions the file/folder/drive you have selected. For instance, if you've selected a folder inside your drive, it will put restrictions only on that selected folder and possibly any files those are inside of it. Those who can access the drive depend on the permissions you've set.

2.10 Encrypt your email and data

There are several ways to encrypt data, and several tools that can be added to mail programs that will even do it for you. Not all are compatible with each other so we'll just talk about encrypting by hand, using the underlying technology that many, though not all, of those tools use Gnu Privacy Guard or GPG. This technique works with all mail programs. This is command-line tool. Once installed, open a Windows Command Prompt and run the tool from there. It's perhaps easiest to simply "CD" to the directory containing the GPG executables. Alternately you can copy all the "G*.exe" executables to a different directory already on your PATH.

Run "gpg" once, and it will create its storage location for keys, which it refers to as your "key ring". In encryption, the first approach that typically comes to mind is password or phrase encryption. With those techniques, a password is used



```
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user
ID
from the Real Name, Comment and E-mail Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: FOSSwire Test
E-mail address: peter@fosswire.com
Comment:
You selected this USER-ID:
    "FOSSwire Test <peter@fosswire.com>"

Change (N)ame, (C)omment, (E)-mail or (O)kay/(Q)uit?
```

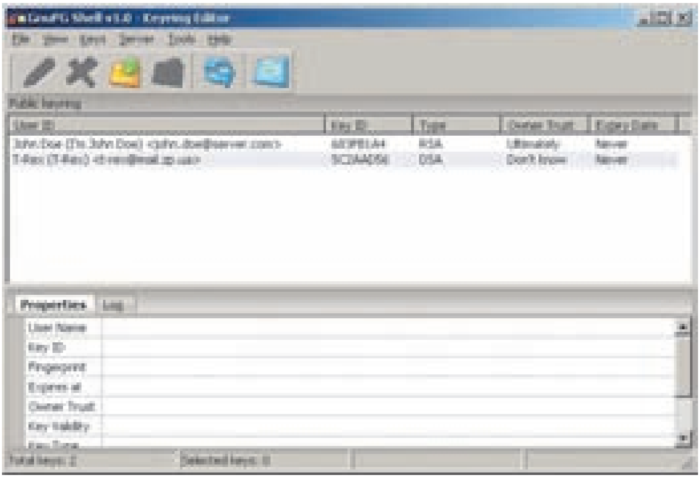
Using public key encryption

to encrypt the data, and then must be supplied again to decrypt it. The data without the password is theoretically useless, but anyone with the password can decrypt it.

Public Key encryption uses a different style of algorithm. To begin with, you'll generate two matching "keys"; a public key, and a private key. The characteristic of these keys is such that data encrypted with one can only be decrypted with the other. By generating a public/private key pair, someone can encrypt data using the public key that can only be decrypted using the associated private key. If all you have is the public key, you can't even decrypt what you've just encrypted.

The intended recipient needs to generate a public/private key pair. In the Windows Command Prompt, enter gpg --gen-key. First select which kind of key you want, as well as the keysize (you can also accept the default which is 2048 bits). You must also specify when the key will expire and to whose email and name it will be valid. Finally, enter a passphrase to protect your key and GPG will begin compiling a key pair. During the process, it's a good idea to move the mouse or access your drives as this will give the random number generator more info to work with.

At this point your secret key and your public key have been generated, and placed on your key ring (which can be managed via the key ring editor). In order to get the public key to the person who wants to encrypt your data, you'll need to export it:



User ID	Key ID	Type	Owner Trust	Expiry Date
John Doe (Tis John Doe) <john.doe@server.com>	6E0FB1A4	RSA	Ultimately	Never
T-Rex (T-Rex) <t-rex@mail.zp.ua>	5C2AAD56	DSA	Don't know	Never

User Name	
Key ID	
Fingerprint	
Expires at	
Owner Trust	
Key Validity	
Key Type	

An example Keyring editor

```
c:\>gpg -a --export example@xyz.com >mykey.pub
```

This creates “mykey.pub”, a text file that contains your public key. You can now mail this to the person who’s going to encrypt data to be sent to you, or post it publicly if you like.

In order to encrypt data, the sender will have to install GPG as above. They don’t need to create their own public/private key pair in order to encrypt your data. All they need is the public key you created above, and made available to them somehow. Start by “importing” your public key onto their key ring.

Note the dire warning about making sure you know whose key you’re dealing with at the end of the encryption process. There are ways to modulate this message but for now, assume you can trust the receiver. The result of this example operation is “example.xls.asc”. This text file is your encrypted data. You can email it with confidence to the intended recipient, knowing that only they can decrypt it with their matching private key.

So you’ve passed your public key to the sender, they’ve used it to encrypt your sensitive data, and have emailed you the encrypted results. From your mail client, save the encrypted data to a text file - it’s ok to leave headers and such in the file, the decryption program will ignore it.

To decrypt, you’ll do this:

```
c:\>gpg -o example.xls --decrypt example.
xls.asc
```

The “-o” parameter specifies the name of the decrypted file to create. Note that you still need to enter the passphrase for your private key. This is only an additional layer of protection on your private key. Without a passphrase, anyone who gains access to your private key would be able to decrypt any messages intended for you.

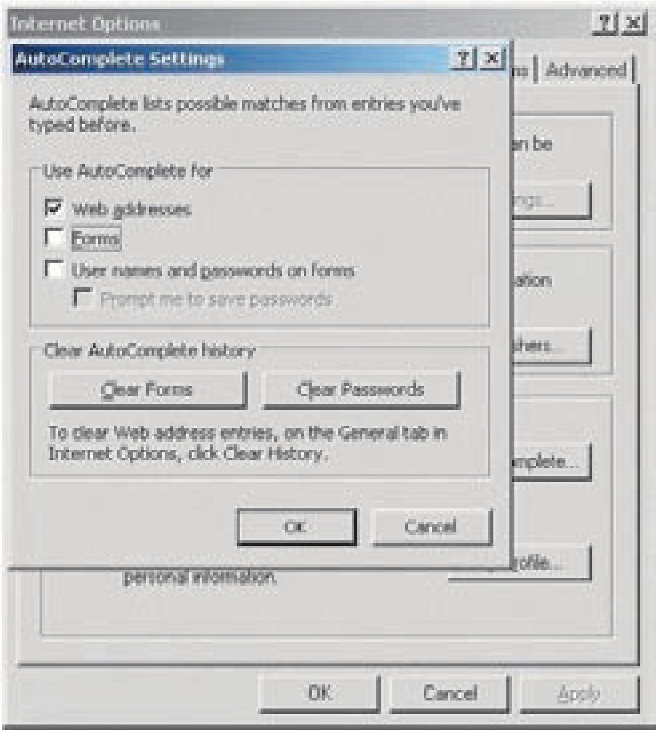
The weakest link in this process if your private key. If an unauthorized person gets a copy or can guess the passphrase on it, your security will have been breached. So it all boils down to this: Keep your private key secure.

3 Cyber Cafes

3.1 Elementary Precautions

Cyber cafes are very popular in India. The technology revolution ensures that everyone has a use for the internet. Computer costs and casual use have since facilitated the growth of cyber cafes. People mainly use cyber cafes for browsing the internet, checking their mail and chatting.

The first important rule is to never tell the cyber cafe owner (or anyone else for that matter) your email ID and password to check your mail. This may sound dumb but keep in mind that many old folks and small kids have no idea about the risks of spam and information theft. Email IDs and passwords should



AutoComplete lists possible matches from entries you've typed before.

Use AutoComplete for

☑ Web addresses

□ Forms

□ User names and passwords on forms

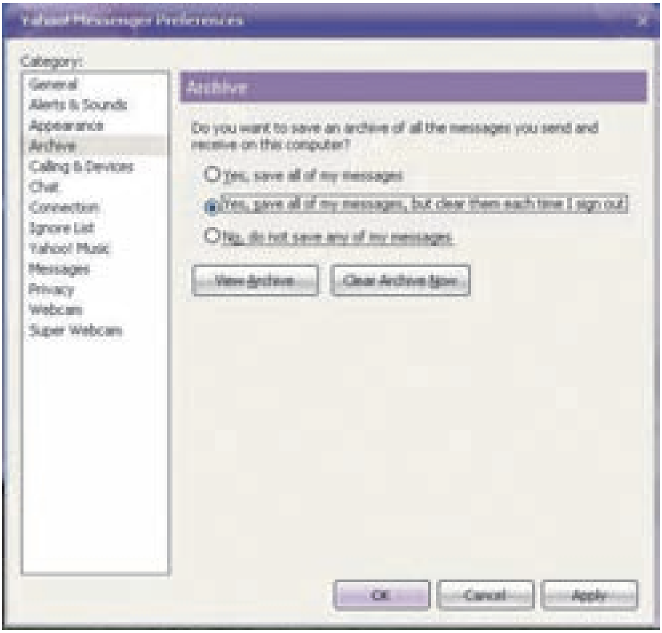
□ Prompt me to save passwords

Clear AutoComplete history

To clear Web address entries, on the General tab in Internet Options, click Clear History.

personal information.

Turn off the autocomplete option when browsing on public computers



Yahoo! Messenger Preferences

Category:

- General
- Alerts & Sounds
- Appearance
- Archive
- Calling & Devices
- Chat
- Connection
- Ignore List
- Yahoo! Music
- Messages
- Privacy
- Webcam
- Super Webcam

Archive

Do you want to save an archive of all the messages you send and receive on this computer?

○ Yes, save all of my messages

● Yes, save all of my messages, but clear them each time I sign out

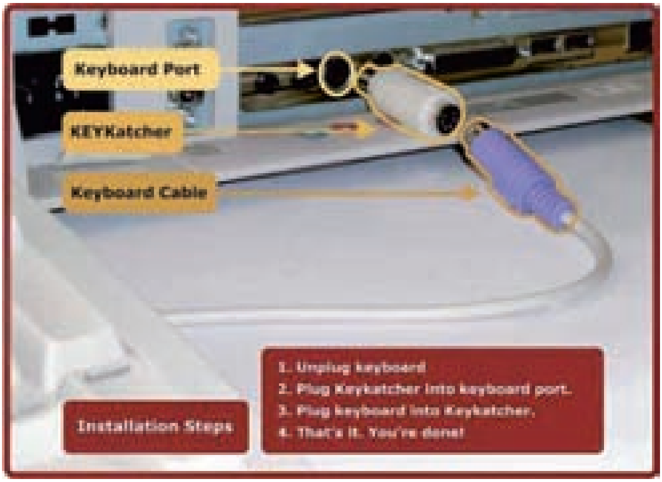
○ No, do not save any of my messages

Disable options that allow archiving of messages as text files

always be entered by their owners. At most, they should ask for guidance to the log-in screen to enter their details personally.

Another important rule is the practice of people coming with their floppies, CDs or pen-drives to send their resumes via email. Usually, the individual computers have neither floppy nor CD drives (and some places prohibit independent use of pen-drives for security reasons). The media is hence run through the server itself before being transferred to the relevant individual's PC. After sending these documents, the user forgets about deleting the documents on the original server. More than simply emptying the Recycle Bin, you should ensure the cyber cafe has a file shredder program to properly delete the files. Resumes contain many personal details, and you should avoid all risk of these being exposed.

Other options you should be aware of when surfing include disabling the option for "Remember my ID on this Computer"


Keyboard Port
KEYKatcher
Keyboard Cable
Installation Steps
1. Unplug keyboard
2. Plug Keykatcher into keyboard port.
3. Plug keyboard into Keykatcher.
4. That's it. You're done!

Keyloggers can be used to capture your personal information by capturing your keystrokes

when surfing. Make sure to turn off the autocomplete option in the browser. This can be done by accessing the `Tools > Internet Options > Autocomplete tab` in Internet Explorer and `Tools > Options > Privacy > Password tab` in Firefox. There are also options to clear your private history / temporary internet files while surfing in case you don't want your browsing history known.

Always make sure to logout properly when using messenger software or mail accounts. Some people make the mistake with IM software in simply closing the program, which does not shut it down but minimizes it into the system tray. This should be taken care of to ensure the next user doesn't use your IM account as he wishes. As specified above, make sure the options for remembering passwords or IDs is disabled. You should also take care to disable options that allow archiving of messages as text files. This helps in keeping conversations private and personal info usually shared online safe.

Finally, whenever you go to a cyber cafe, ensure it has the most up-to date anti-virus and spyware definitions. These will help root out Trojan horses and keyloggers responsible for tracking your activity and recording your passwords/IDs.

3.2 Bypassing Keybloggers

A keylogger is basically spyware. As indicated by its namesake, it “logs” or records your keystrokes. When you type in your username or password, this information is logged and made available to the hacker. Keyloggers can either be physical or software-based, the latter being more difficult to detect.

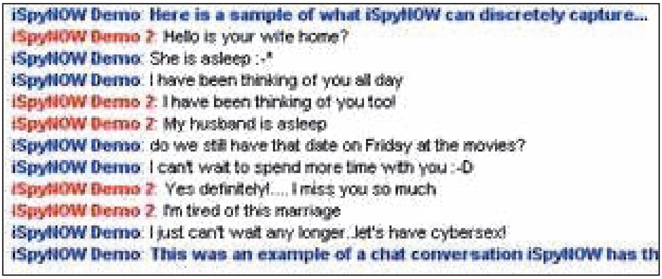
A keylogger works in several different ways:

- Each keystroke is recorded and immediately dispatched to some remote listener over the internet.
- Keystrokes are collected in a temporary file, which is then periodically uploaded to the author’s location over the internet.
- The keystrokes are collected in a temporary file, but much like a spam bot, can listen for and receive instructions from the author. The logger could thus upload the collected information when requested.
- The collected keystrokes could never be uploaded.

Instead, if someone has remote access to your machine, or even physical access to your machine, they could simply come by and copy the information manually.

- Finally, the information may not even be kept on your machine. There are hardware keyloggers that include a little flash memory and can be quickly inserted in between keyboard and computer to capture all the data. After installing, the person behind it stops by and picks up the device containing all your information.

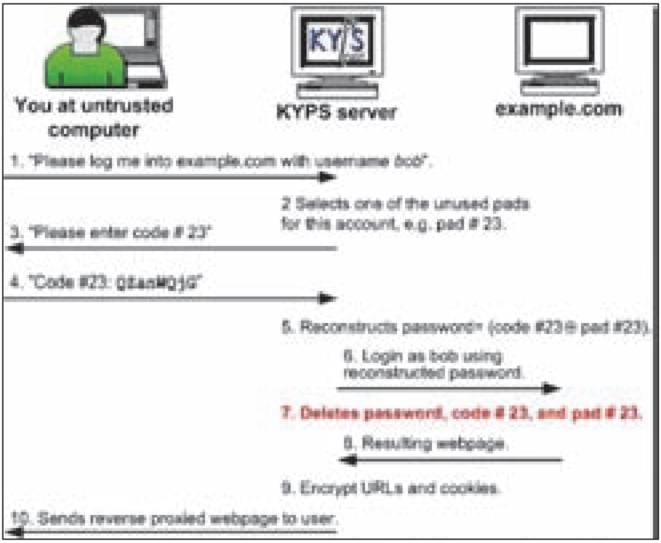
There are two basic methods for bypassing keyloggers, both which involve confusing the logger with random keystrokes. The first, when you need to enter a username or password, is to randomly insert irrelevant numbers and letters in between the same. Once entered, just select the random bits with the mouse and delete them before logging in. The second is for fooling keyloggers that capture all keystrokes and not just those typed in the password box. Enter your info randomly across the browser and search bars along with random numbers and letters. When you wish to log in, simply copy and paste the relevant bits into the log-in boxes. Another option, on-screen keyboards, will be explained in a later chapter.



```
iSpyNOW Demo: Here is a sample of what iSpyNOW can discretely capture...
iSpyNOW Demo 2: Hello is your wife home?
iSpyNOW Demo: She is asleep :-*
iSpyNOW Demo: I have been thinking of you all day
iSpyNOW Demo 2: I have been thinking of you too!
iSpyNOW Demo 2: My husband is asleep
iSpyNOW Demo: do we still have that date on Friday at the movies?
iSpyNOW Demo: I can't wait to spend more time with you :-D
iSpyNOW Demo 2:  Yes definitely!.... I miss you so much
iSpyNOW Demo 2: I'm tired of this marriage
iSpyNOW Demo: I just can't wait any longer..let's have cybersex!
iSpyNOW Demo: This was an example of a chat conversation iSpyNOW has th
```

keep online relationships in the online realm

You can also use KYPS, a reverse proxy server that takes a password, encrypts into a one-time code, printed from the KYPS web site that can be used to log into any computer safely. After being decrypted by the KYPS system and logging in, it deletes the one time code as a password. KYPS also acts as a normal proxy to protect


KYS
You at untrusted computer
KYPS server
example.com
1. "Please log me into example.com with username bob".
2 Selects one of the unused pads for this account, e.g. pad # 23.
3. "Please enter code # 23"
4. "Code #23: Q$an#QjG"
5. Reconstructs password= (code #23⊕ pad #23).
6. Login as bob using reconstructed password.
7. Deletes password, code # 23, and pad # 23.
8. Resulting webpage.
9. Encrypt URLs and cookies.
10. Sends reverse proxied webpage to user.

KYPS, a reverse proxy server can be used to login to any computer safely

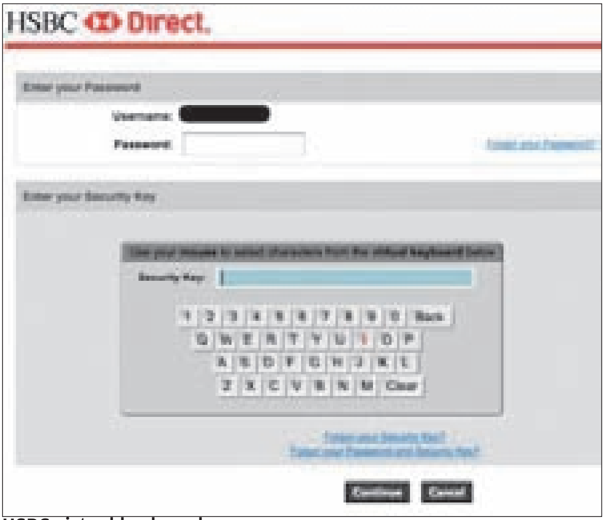
your browsing history. When browsing, it displays the KYPS URL along with random characters and symbols to maximise security.

The "Work Offline" option shouldn't be relied on too often. This feature is specific to Internet Explorer or the application with that function, and it's not too hard for a keylogger to bypass something so narrow. Also, even if you physically pulled out the internet connection wire from your PC, only the first of the above approaches is rendered harmless. The keylogger can still quietly collect the data and transmit it when a connection is available.

As such, there is no way to be 100% careful against keyloggers. It depends on specific keyloggers most of the time. However, you should always remain cautious when entering a cyber cafe.

3.3 Safe Surging

Safe surfing doesn't simply refer to tips for kids surfing online. Internet usage across the globe is ever growing. Hence it's



HSBC Direct

Enter your Password

Username: [redacted]

Password:

Forgot your Password?

Enter your Security Key

Use your mouse to select characters from the virtual keyboard below

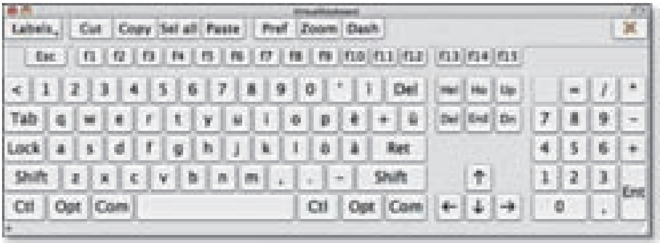
Security Key:

HSBC virtual keyboard

necessary for everyone to remember a few basics while surfing the net. They can easily prevent you from being the victim of some scam or being taken in by someone who appears trustworthy.

The most elementary precaution of net surfing is to not give out any of your personal information. This includes your name, address, credit card numbers, phone number and passwords. Remain as anonymous as possible, as often as possible. Remember, most credible sites and services don't require this information for simple surfing. If one requests any of the above details, then beware. If cheating on the internet weren't so easy, phishing wouldn't be as common as it is today.

Think carefully before creating an email address or screen name. Avoid identifying whether you're a male or female. When entering a chat room, make sure to adjust a nickname substantially different from your screen name. If a conversation makes you uncomfortable, you can leave without worrying about having your email tracked through your screen name. Friends should also set up private chat rooms when chatting with people they know rather than discussing things in the open. Keep most


Labels Cut Copy Sel all Paste Pref Zoom Dash
Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 F13 F14 F15
< 1 2 3 4 5 6 7 8 9 0 ' Del
Tab q w e r t y u i o p + Del End Dn 7 8 9 -
Lock a s d f g h j k l Ret 4 5 6 +
Shift z x c v b n m , . - Shift 1 2 3 Ent
Ctl Opt Com Ctl Opt Com ← ↓ → 0 .

Virtual keyboard

online friendships in the online realm. If you really wish to meet an online friend in the real world, always make sure it's in a public place and you're in the company of friends and family. Remember that it's very easy for someone to be someone they're not, age-wise and what not.

Read the fine print on a web page you visit. Even if you conform to the law, saying 'yes' on some of these pages is as good as giving your personal signature. Confirm that you won't be receiving any unnecessary spam or that your contact details are not circulated with other sites. Avoid any pages of a dubious nature, especially ones that ask for your personal details especially if you think it's unnecessary. Any pop-ups that prompt you to click on them could be spyware.

Always have the latest security software and remember to keep it updated. If you ever receive an anonymous attachment or email, delete it right away without opening it. Spam blockers are especially important but don't neglect having anti-virus and anti-spyware software installed on your PC. Firewalls are also good for preventing any one from illegally accessing your PC from the outside. However, always remember that these are safety measures. Only if you apply a liberal amount of common sense will they be truly effective. Not even the most up-to date software can save you when you're willingly giving out personal details.

3.4 Using on-screen keyboards

An on-screen or virtual keyboard is a software component that allows a user to enter characters into a keyboard displayed on the display. It is used by disabled users who cannot operate a physical keyboard. It has also emerged as a key method for reducing keystroke logging. There are two types of on-screen keyboards: Program to program or non-web keyboards and web-based keyboards.

Non-web keyboards are the weaker of the two. These keyboards (such as the onscreen keyboard that comes with Microsoft Windows XP) send keyboard event messages to the external target program to type text. Every software keylogger can log these typed characters from one program to another. This problem persists with both third party and first party virtual keyboards. There are other means for protection in this case, like dragging and dropping the password from the on-screen keyboard to the target program.

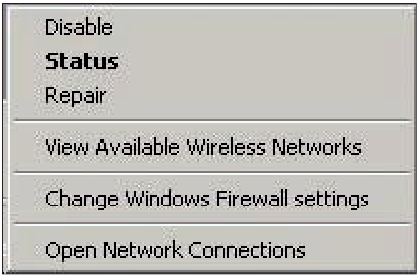
Web-based keyboards offer more protection. Some commercial keylogging programs thankfully do not record typing on a web-based virtual keyboard. Many banks like HSBC use a virtual keyboard for password entry.

Technically, it's possible for a malware to monitor the display and mouse to obtain the data entered via virtual keyboard. Screenshot recorders take quick and regular photographs of the desktop, and can effectively obtain the data via virtual keyboard. This is significantly harder compared to monitoring real keystrokes. If the recorder is not fast enough, it cannot effectively capture all the mouse clicks displayed.

On-screen keyboard use can also increase the risk of password disclosure by shoulder surfing. An observer can watch the screen easily (and less suspiciously) than the keyboard and see which characters the mouse moves to. Some implementations of the on-screen keyboard give visual feedback of the key clicked by, say, changing its colour briefly. This makes it much easier for an observer to read the data from the screen. This implementation may leave the focus on the most recently clicked key until the next virtual key is clicked. This allows the observer time to read each character even after the mouse starts moving to the next character. Finally, a user may not be able to point and click as fast as they could type on a keyboard, thus making it easier for the observer. This especially becomes a problem in cyber cafes that do not feature separate cubicles for privacy.

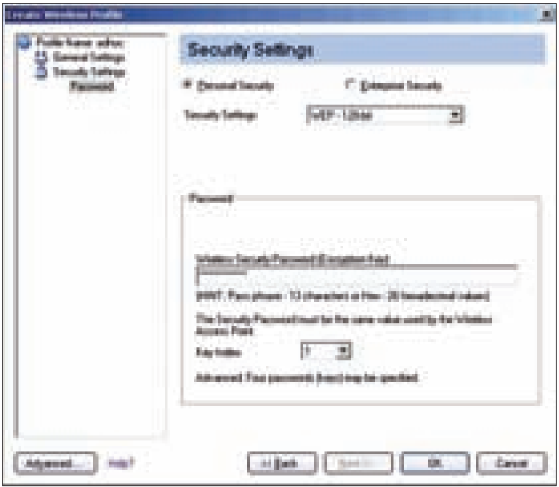
Fortunately, software exists to combat some of these problems. Corallo Software's Virtual Keyboard application provides an option to make the keyboard transparent (0-90%) when you move the cursor away. It can handle command-key combinations, modifier key-click combinations and auto-key repeat. The shareware program is applicable for 14 days before registration but a Lite freeware version is also available. Both have support for all operating systems, including Mac OS 8 and Intel-based Macs.

4.1 Protection with intrusion


Disable
Status
Repair
View Available Wireless Networks
Change Windows Firewall settings
Open Network Connections

Finding available networks

WiFi is a Peer to Peer (P2P) file sharing service just like Bluetooth. Anyone can get into your connection if your WiFi is not secure. Before securing your WiFi, it's important to check how secure it really is. Right click on the small wireless network icon on your Task Bar. Select "View Available Wireless Networks" from the available menu. There are usually two types of networks: Security-enabled wireless network and unsecured wireless network. The former needs a security key (a password most times) to access. An unsecured wireless network can be logged into without a password. An insecure network is roughly equal to an insecure WiFi router, so take the following steps to secure your WiFi network.



Creating a wireless profile

The Router/Access point is the main config unit. Whoever infiltrates this, can change security settings like passwords, encryptions and more. Most routers have default passwords and SSID (Service Set Identification), so make sure to change the passwords to make the entire system secure. The SSID identifies your router. Most companies use default ones which come with the router like Linksys, wireless or WLAN or they their company name. Choose a more secure password, like a random combination of letters and numbers. The most important part is to disable SSID broadcasting which transmits the SSID to everyone in range. It is recommended that the encryption keys and the SSID are changed very frequently.

Remote management is used to access/modify the configuration of Router/Access point from any client machines using login ID and password. It's recommended this is disabled. For any configuration, have one connect physically to a machine via a network cable. If your WiFi offers WPA2 encryption, then use it (if the router does not support it, you can choose WPA or WEP). Then make sure a password is assigned which is more or less invulnerable to dictionary attacks and choose the highest available encryption option (232->104->40).

Most of us use WiFi at home or in the office. It is recommended to lower the transmit level and reduce the area of the WLAN covers. This will help in providing WiFi signals to a specified area and lower the risk of intrusions.

Ad-Hoc mode allows for direct communication of all devices connected to the wireless LAN through the access point/router. Disable Ad-Hoc when available. Also turn off Broadcast ping on the access point/router. This will make your router invisible to 802.11b analysis tools. Most WiFi is kept on for 24 hours. It's recommended to switch off the WiFi router when not in use.

4.2 Protect Bluetooth intrusions

Peer to peer (P2P) file sharing has become popular but not without a heightened amount of threats. Users often receive files from unknown senders which can lead to security problems, especially with music and media sharing. Like any personal computer, these files can be malware that infiltrate and cause havoc within your laptop. The entry points for intruders are the very same open ports that allow you to transfer files.

Make sure to only perform file transfers from trusted sources. Besides reducing the risk of downloaded files having malware, there's an element of accountability. Hence you get a better response if there is a problem. Keep an anti-virus scanner handy when transferring files over Bluetooth or P2P. While it may slow down the transfers, it's definitely much safer.

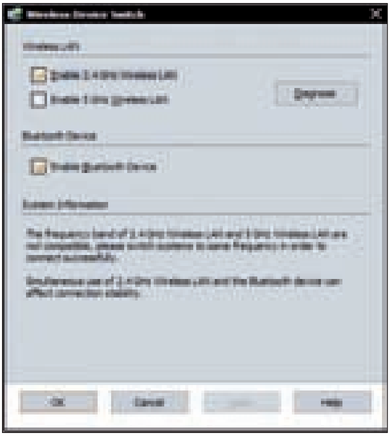
Sometimes, after you discover an intrusion, you are left with no option but to format your hard drive and reinstall your operating system. Keep backups of important data so you can restore your important files quickly. Typical backup methods apply here, and just like before, keep your info in a secure location separate from your laptop to ensure it remains unaffected.

Remember to turn off Bluetooth when you're not using it. To turn off Bluetooth on a Windows Pocket PC enabled device:

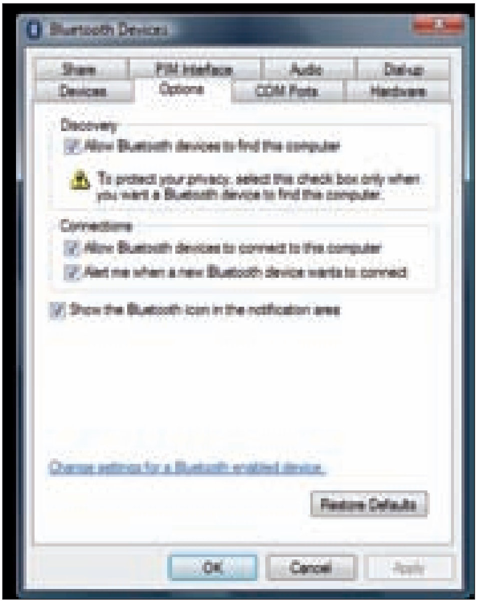
1. Click on the Windows icon in the top left corner of the screen and choose Settings.
2. In Settings, choose Connections and then Bluetooth.
3. If you see that Bluetooth is turned on, click on the Turn Off button.

You can also use the passkey option to eliminate unwanted connections. Only people who have a personal password can connect to your device. This way, you are notified if anybody tries to establish a connection with you. To use passkey, click on the Bluetooth Manager and select Passkey.

You can protect your mobile device by preventing other devices from finding you and connecting to you. This way, you can still connect to other devices, but they cannot connect to you first. This protects you from sneak attacks. To disable discovery on a



Turning Bluetooth on or off



Discovery

☑ Allow Bluetooth devices to find this computer

⚠ To protect your privacy, select this check box only when you want a Bluetooth device to find this computer.

Connections

☑ Allow Bluetooth devices to connect to this computer

☑ Alert me when a new Bluetooth device wants to connect

☑ Show the Bluetooth icon in the notification area

Change settings for a Bluetooth enabled device.

You can disable discovery from here

Windows Pocket PC-enabled device:

1. Click on the Windows icon in the top left corner of the screen and choose Settings.
2. In Settings, choose Connections and then Bluetooth.
3. Click on Accessibility to get to the screen shown in the figure below.
4. Uncheck the "Allow other devices to connect" and "Other devices can discover me" boxes.

Finally, make sure the public network you are accessing is secure. If a network does not ask you to identify yourself with a password, then beware. Just about anyone can log onto the same network as anonymously. It's better to avoid unfamiliar networks than to risk any attacks.

4.3 Securely share Wi-Fi connectivity with other devices

We've gone over the risks of using a Wi-Fi network that is insecure. But what if you want to connect with devices and do so securely? This is usually the case when one wants to

1. Provide wireless internet to a group of users who cannot access a restricted part of your Local Area Network (LAN). This can be called public access wireless internet users (even though it may not permit the general public to access the LAN).

2. The restricted part of your LAN contains your NAS, some PCs, and other devices. The restricted part needs to exchange files among other devices on the restricted part but not with devices on the public access side.

Let's assume that you want to do wireless access on the restricted side. There are two ways to do this that come to mind.

Purchase a router that supports at least 2 LAN subnets via wireless access points. The Adtran Netvanta 3120 with their Netvanta 150 wireless access point will do this; a Motorola WS 2000 will also do this. Configure subnet # 1 for restricted users and give it a subnet like 192.168.10.0/24 (24 means 24 bit subnet mask of 255.255.255.0); configure subnet # 2 for public users ADN give it a subnet like 192.168.20.0/24. Use the MAC address of the restricted devices to permit these devices onto the 192.168.10.0/24 subnet which will automatically put these devices in the proper subnet. All other devices will be automatically sent to 192.168.20.0/24. With separate subnets the 2 groups are separated in their own virtual LANS or VLANS.

Have your existing router and wireless strongly secured including MAC address validation, WPA or WPA2 with strong pre-share key. Note the subnet you have with this router (probably 192.168.0.0 / 24 or 192.168.1.0 / 24; no need to change, just note it. Purchase a second wireless router and give it a different subnet, something like 192.168.20.0/24 and do not provide security on it.

4.4 Prevent “shoulder surfing”

In computer security, shoulder surfing refers to using direct observation techniques, such as looking over someone’s shoulder, to get information. Shoulder surfing is particularly effective in crowded places because it’s relatively easy to observe someone as they enter passwords on a computer, fill out a form or enter their PIN at an automated teller machine (ATM).

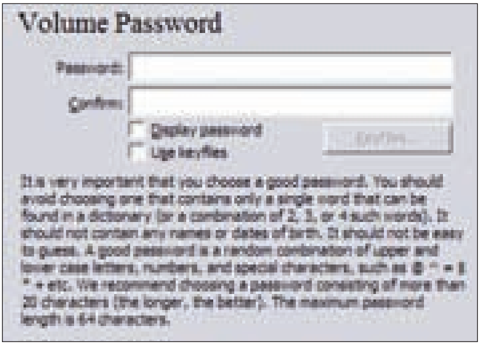
Shoulder surfing can also be done at a distance using binoculars or other vision-enhancing devices. Inexpensive, miniature closed circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry. To prevent shoulder surfing, it is advised to shield paperwork or the keypad from view by using one’s body or cupping one’s hand. When working on a laptop, ensure that your back is to a wall with no open sides close to you or to enter your passwords in a secluded location.

Recent automated teller machines now have a sophisticated display which discourages shoulder surfers. It grows darker beyond a certain viewing angle, and the only way to tell what is displayed on the screen is to stand directly in front of it.

Certain models of credit card readers have the keypad recessed, and employ a rubber shield that surrounds a significant part of the opening towards the keypad. This makes shoulder-surfing significantly harder, as seeing the keypad is limited to a much more direct angle than previous models. Taken further, some keypads alter the physical location of the keys after each key-press. For example the digit 1 may be the upper left on the first press, then moves to the bottom right for the second.

4.5 Encypt your hard drive

Securing computer data through encryption software has become a clear necessity for many businesses and individuals carrying sensitive information on their laptops or USB flash drives. Unfortunately, many people do not encrypt their data because it is not easy to implement in Windows and the learning curve is too high. However, thanks to open source initiatives, you can use a completely free program called TrueCrypt to encrypt an entire hard drive, a USB flash drive, or even create a virtual encrypted disk in a file that acts as a real disk.



Volume Password

Password:

Confirm:

□ Display password

□ Use keyfiles

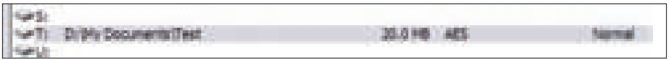
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum password length is 64 characters.

Encrypting a drive's contents

TrueCrypt can create a virtual disk on your computer that will look and feel just like a normal disk on your computer. The "drive" will actually be a file stored on your computer, but it is completely encrypted and secure, so that when you turn off your computer, the data can't be recovered unless you know the correct password. Of course, losing this password means losing your data, so don't forget it under circumstance. It even encrypts the file names and the folder names on the volume. TrueCrypt supports Windows Vista and Windows XP x64. It also runs on Linux and you can open a TrueCrypt volume on any of these platforms.

Once installed, click on Create Volume. Choose Create a Standard TruCrypt Volume. Click Select File, browse to where you want the file stored and type in a name for the file. Next choose the encryption that you want. The default option is the lowest encryption method, AES and the last in the drop down being the highest. Remember, each time something is read from the virtual disk, it has to be decrypted and it will take more time to decrypt if the encryption is stronger.

Next choose the size for your virtual drive. Click Next and now type in a strong password. It is essential you type in a long and complex password so that it cannot be easily cracked. As such, the program asks for a minimum of 20 characters. On the next screen, a random header and master key will be



```
S:
T:   D:\My Documents\Test          20.0 MB   AES          Normal
U:
```

An encrypted drive

generated. Choose the format of the drive and click Format. Finally, click Exit to get back to the main screen. Choose a letter from the drive list and click Select File to pick the volume that you will be mounting. Now click the Mount button at the bottom to “connect” or mount the file to the selected drive letter. You’ll be asked to type in the password that you entered while creating the virtual volume. Click OK and you should see the list updated. Your new drive will now show up in Windows Explorer as a local disk.

Now you can use the drive normally. When you restart or turn off your computer, the drive is dismounted and the drive is inaccessible. When Windows starts, you will have to re-mount the drive with the correct password. You’ll only be asked for the password whenever the computer is started up.

4.6 Theft protection measures

Your laptop is at as great a risk of theft as it is of spyware, Trojans and hackers infecting it. At times, the threat can be greater simply because it’s so easy to have your laptop stolen. If this weren’t the case, airline pilots wouldn’t have laptops with the social security numbers and personal details of some 3600 employees compromised. For all the encryption methods available, there are also ways to prevent your laptop from being stolen.

The number one, easiest, cheapest and most obvious laptop protection technique is to simply be

A security cable

Try stealing this laptop, and you'll probably break the table

aware that it's an easy target for theft. Stay alert at all times. Never leave your laptop alone at a table in a restaurant or public place. Be aware of the unsecure areas from which your laptop could be stolen like for instance, a crowded bus, or when walking home late at night. Just the very thought that you're responsible for something incredibly important is enough most of the time.

A security cable is one of the most popular laptop protection tools. You wrap the cable around an immovable object and insert the locking head through the cable loop. An immovable object can include anything from sinks, around steering wheels, pipes that go into the sink and even the base of the toilet. Even if a thief sneaks into your house when you're asleep, it won't be easy for him to walk in and walk out with your information.

Motion detecting alarms are also available for laptops. Simply attach it to a carry case or laptop, alarm it with the adjoining key pad and it's ready to yell at the slightest bump or jiggle. Remember to keep the batteries fully functional. Many motion detecting alarms are included with security cable nowadays.

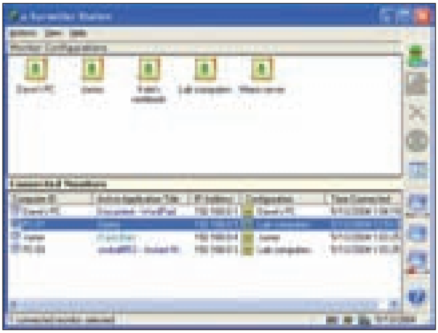
A unique method is Caveo's Anti-Theft PC Cards. They operate by detecting motion, analyzing it to determine whether a threat exists, and implementing responses. They are independent of the computer operating system and operate whether the laptop is on or off. If an armed system is carried beyond a perimeter specified by the user, Caveo Anti-Theft assumes theft and invokes strong responses, including preventing access to the operating system, securing passwords and encryption keys, and sounding an audible alarm (which is optional). This same technology is used by museums to prevent collection theft.

One or more combination of the above technique and tools should be more than enough to ensure necessary laptop protection.

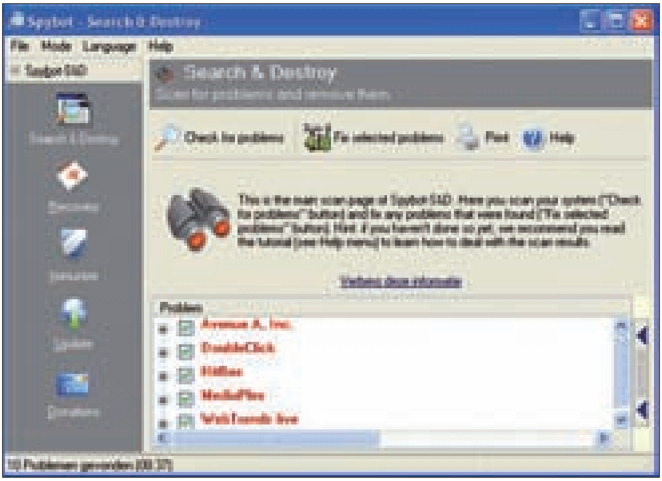
4.7 Firewalls and snoopware protection

Snoopware is malware deployed invisibly in your system. The snoop software can store just about anything that you do in your computer. Snoopware can store all the keystrokes you make. Snoopware can also get all your login information. Snoopware can store and log all your typed URLs, store credit card numbers and can also log all the windows you opened. It can also take screenshots of your system at specified intervals. Above all, snoopware can send all these data to any remote location, automatically, using your Internet connection (which can be combated using firewalls).

Snoopware mainly employed for monitoring employee activities and activities of children on the net. However, it's mainly employed for malicious purposes and can be considered in the same league as spyware. Besides, even if the software



Monitoring activity



This is the main scan-page of Spybot-S&D. Here you scan your system ("Check for problems" button) and fix any problems that were found ("Fix selected problems" button). Hint: if you haven't done so yet, we recommend you read the tutorial (see Help menu) to learn how to deal with the scan results.

[illegible]

- ☑ Avenue A, Inc.
- ☑ DoubleClick
- ☑ HitBox
- ☑ MediaPlex
- ☑ WebTrends live

10 Problemen gevonden (00:37)

Spybot can prevent malware from spying on you

is there without your permission at work, it's ultimately you who decides whether you want your activities to be known or not. If you are very hesitant in revealing your private and important data, it becomes essential to fight back and snoop out the snoopware. Thankfully there is anti-snoopware software that will help you find out the snoopware in your system and also clean them from your computer.

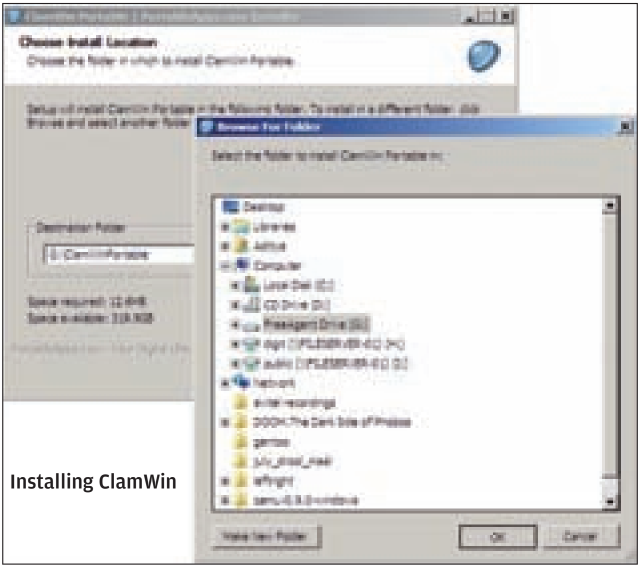
Your first step is to download a good anti-spyware program (Spybot: Search and Destroy will work nicely). Scan your computer for spyware, which can range from registry keys, cookies, and other snoopware and loggers installed in your system. Remove the installed spywares and cookies using Spybot. Of course, even if you remove these snooping programs from your computer, there is no guarantee it won't come back. Like an anti-virus scanner, schedule daily updates and scans to keep your system clean, safe and up to date. There are plenty of new snoopware being developed on a daily basis, so Spybot's easy and secure updating comes in handy. Firewalls are most useful for denying any one remote access into your computer. Also see the section on keyloggers for effectively combating snoopware that records your keystrokes.

Portable Devices

Portable devices, such as portable hard drives and thumb drives are a very common entry points for viruses and trojans. A stint at a cybercafé, or using your portable device at office and home is very likely to infect your computers. There are a few simple steps that can be taken to protect your portable drives from common Viruses and Trojans. The method discussed below will work even if the account on the computer you are working with does not have administrator privileges.

5.1 Protect External data from Viruses and Worms

The simplest way to protect your portable device from infection is to use a portable antivirus. The most robust portable antivirus solution is ClamWin, an open source anti-virus. However, ClamWin is not as good on performance and detection as some of its commercial counterparts. You will have to download regular updates, to make sure that the anti-virus is ready to tackle the latest threats. Also, ClamWin does not include any kind of on-access scanning, which means that you can take



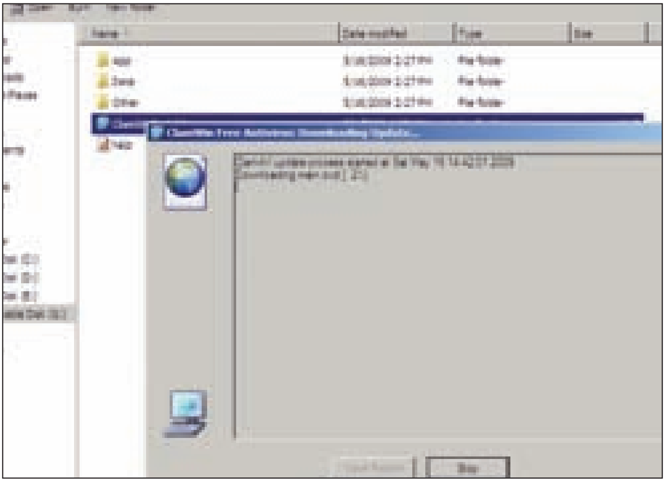
Installing ClamWin

care of the virus problem only after the infection.

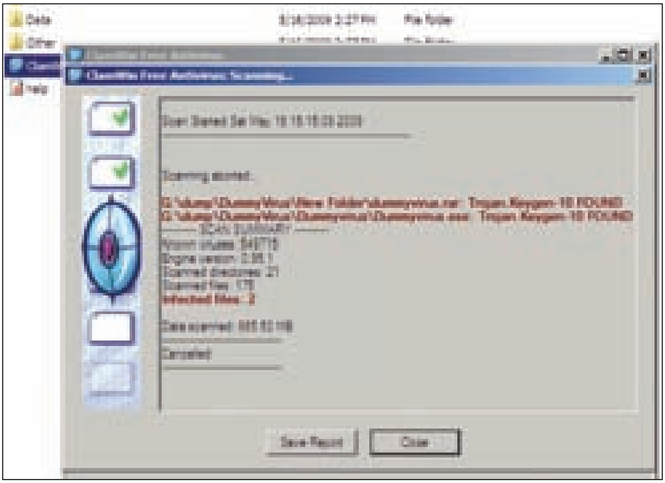
The portable version of ClamWin can be downloaded from portableapps.com. Once the installation client is downloaded, you will have to connect your portable drive to the computer. You will have to connect an external hard drive or other portable device at this point to the computer. Install the application, and select the portable location for installation. The application won't appear in the Program Files listing, so every time you want to run it, you have to navigate to the portable device using Explorer, and manually click on the ClamWinPortable.exe file to start ClamWin up.

The first time you start ClamWin, you will have to download and install the virus definitions. These help ClamWin stay up to date with the latest threats, and handle them. The first time this is done, it will take some time, depending on your internet speed. After the first time the updates are downloaded, subsequent definition updates take comparatively less time. Also, as ClamWin is a portable software, you can copy and paste the ClamWin folder in a number of portable locations, after the virus definitions have been updated.

Click on scan, and select the device you want to scan. This can include the device that you have the anti-virus in, or the host computer. Scanning will take some time, and then a report



Clamwin database update



```
Scan Started Sat May 16 15:15:03 2009

Scanning aborted.
G:\dump\DummyVirus\New Folder\dummyvirus.rar: Trojan.Keygen-18 FOUND
G:\dump\DummyVirus\Dummyvirus\Dummyvirus.exe: Trojan.Keygen-18 FOUND
----------- SCAN SUMMARY -----------
Known viruses: 541775
Engine version: 0.95.1
Scanned directories: 21
Scanned files: 175
Infected files: 2

Data scanned: 555.52 MB

Cancelled
```

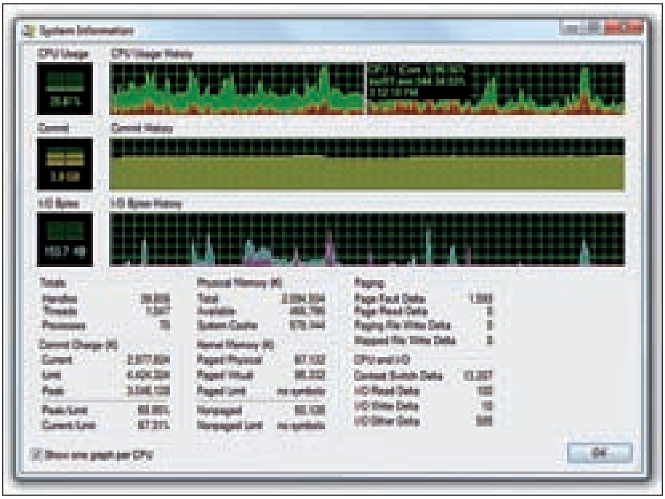
Identifying viruses in Clamwin

of all found threats will be posted on the screen.

There is a simple method for on-access protection, on any location with access to the internet. This however, requires you to be aware of the standard processes that run on the host computer. There is a tool known as Process Explorer. Process Explorer, is an alternative to the Windows Task Manager, with a few more nifty features thrown in. The advantage that Process Explorer has over Windows Task Manager is that you can pause troublesome processes instead of halting them. Many viruses, Trojans and worms are written in such a way that once the process they are running is closed down, they are immediately restarted. Process Explorer merely freezes these processes, with effect that they cannot do anything harmful, or spread to other devices.

There is a portable version of Process Explorer, that can be taken around in a USB drive. Another alternative is to run Process Explorer live, from the internet, which can be done at **http://live.sysinternals.com/procexp.exe**.

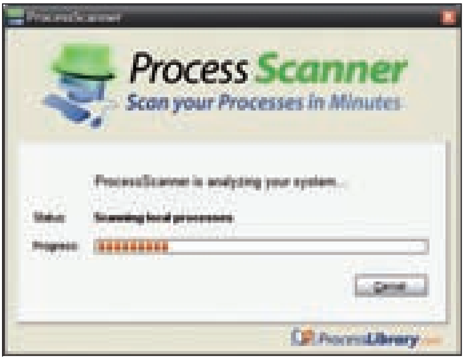
This however requires a fair idea of the harmful processes that you have to watch out for and stop. Just head over to www.processlibrary.com, and you will get a good idea of what processes to watch out for. The most dangerous processes at any



Process Explorer showing the dll and process hierarchy

point of time are listed on the front page itself. You can search for suspicious processes, and find out why they are running, and what they are doing on the computer.

Process Library also offers a small freeware utility that let's you scan all the processes running on the computer for potential threats. This software is available at www.processlibrary.com/processscan. Once the scan is completed, the program communicates with the Process Library servers, and throws up a HTML page with the scan results. Look in the recommendation column for advice on what to do. If you want to rid the host computer of the viruses or worms, you will have to go ahead



ProcessScanner is analyzing your system...

Status: Scanning local processes

Progress:

Process scanner at work

and use an anti-virus. However, if you merely want to safely use your portable memory, use Process Explorer to halt the processes that were alerted by the process scan, and proceed by plugging in the portable storage device.

5.2 Securely carry personal passwords

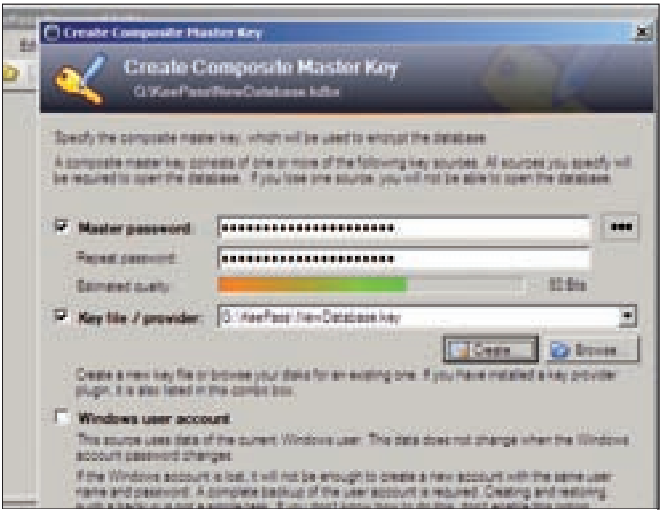
There is a concept known as a “life password”, which is a common tendency amongst computer users. Most people use the same password for all the websites that they use, including forums, social networking sites, image hosting sites and for the whole host of services that Web 2.0 has to offer. This is actually a very risky thing to do, as if a single site gets compromised, or you are misled into signing up on a bogus website, all your accounts are compromised. Your e-mail account is a step away from your financial details, which are enough to scam you. Another, marginally more secure approach that people have is to use high-level passwords for the more sensitive sites, and low-level passwords for all the other websites that they frequent. This too, is not as secure as having a different password for different sites.

The total number of passwords a modern computer user has to keep track of, can quickly get very complicated and hard to manage. For this purpose, people use a password “safehouse”, such as KeyPass, to keep their passwords secure and available at any point of time. KeyPass stores all the passwords for all your accounts in one secure location. The passwords are stored in a database, for retrieval whenever necessary. KeyPass encrypts the files with the passwords that it stores, so it would take considerable time and effort to decrypt the password file, even if the attacker has a lot of computer resources at his disposal. It is possible to choose a combination of protection for your passwords, that all the present computing power allocated to cracking the encrypted text file for the rest of the lifetime of the universe would not be able to crack it. KeyPass is very secure, but the users will have to be careful of two things, the master password to access the password database, and the key file, if the user decides to make one. A keyfile is a block of randomly generated data, that is used to codify the passwords, and to decode them when they are to be retrieved.

The benefits of using KeyPass are twofold. Apart from securely storing all the data in an encrypted database, KeyPass can be used to enter in login and password information automatically. In case the computer you are using has a software or hardware keylogger installed, to monitor internet usage and extract login details for accounts, then KeyPass is very effective at going around such keyloggers. In fact, KeyPass uses a process called obfuscation, that sends a strong of random characters to any keylogger, and in that sense is more effective than using a virtual keyboard.

The first time you start up KeyPass, you will have to set it up in a number of ways. On first run of the software, you will have to choose two key aspects of your security. The first is the master password, which gives you access to all the passwords.

The longer the master password, the harder it is to crack. Remember that a lot of intrusion occurs from people the victims know of in real life. So choose something that people who know you cannot guess as being your password. Also, keep its length above 12 characters at least, and use capitalisation, numerals and symbols. Once a password is created, KeyPass throws up



Create Composite Master Key

Create Composite Master Key
[illegible]

Specify the composite master key, which will be used to encrypt the database.

A composite master key consists of one or more of the following key sources. All sources you specify will be required to open the database. If you lose one source, you will not be able to open the database.

☑ Master password: ••••••••••••••••••••••••

Repeat password: ••••••••••••••••••••••••

Estimated quality: [illegible]

☑ Key file / provider: [illegible]

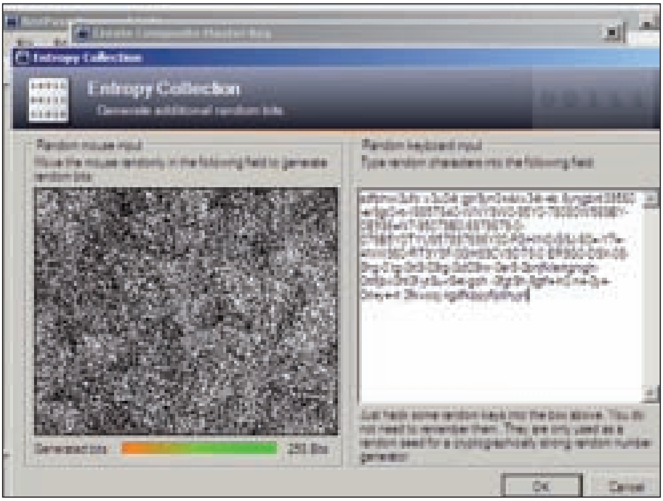
Create a new key file or browse your disks for an existing one. If you have installed a key provider plugin, it is also listed in the combo box.

□ Windows user account

This source uses data of the current Windows user. The data does not change when the Windows account password changes.

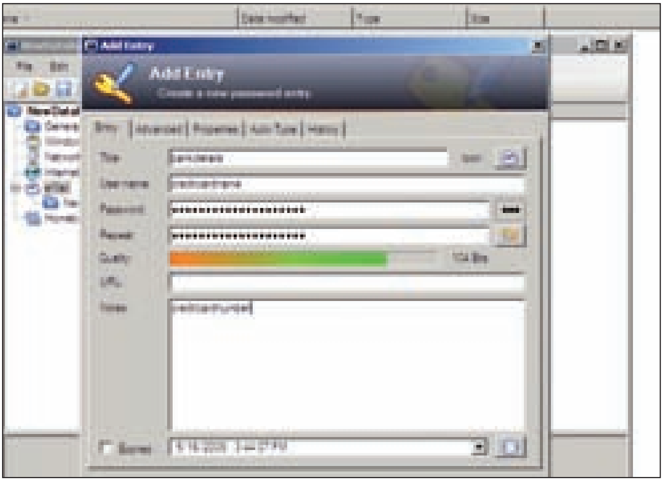
If the Windows account is lost, it will not be enough to create a new account with the same user name and password. A complete backup of the user account is required. Creating and restoring [illegible]

Adding a new database in KeyPass



Generating a keyfile using random data

a "strength" of the password, which is a measure of how tough the password is to crack using brute force methods. Anything over the 50 bit strength is good enough for most purposes. The

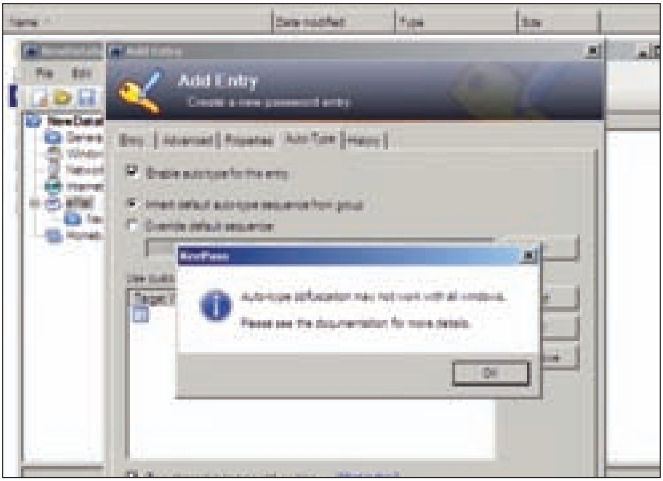


Adding details to KeyPass

second, is the keyfile. A keyfile is not strictly necessary, but is a far more secure way of encrypting your data than the master password. Say your master password is even 20 characters in length, which is very difficult to remember and very long, brute force efforts can still break through the password. “Brute Force” or “Dictionary” approaches to password cracking use every possible combination of letters and numbers to get in, and while time consuming and laborious, it is very efficient. This is where the added security of a keyfile comes in.

Keyfiles use incredibly long strings of random data, and are tougher, if not impossible, to crack using brute force methods.

KeyPass generates the key file for you, if you choose to go for one. There are two methods for generating the keyfile, and they appear side by side in one window. The option on the right allows you to move the mouse randomly over a field. The second option lets you key in a string of random characters. Both these approaches are preferred over a computer approach at generating a random key, because computers have a very limited ability at generating truly random data. The erratic movements of the human is a far more random element, and therefore a stronger source of random data than what the computer can generate. It is generally preferable to use the mouse



Enabling obfuscation in KeyPass

movement as a mode of input rather than typing out random keys, as typing out random keys wont be as random as moving the mouse in a random fashion.

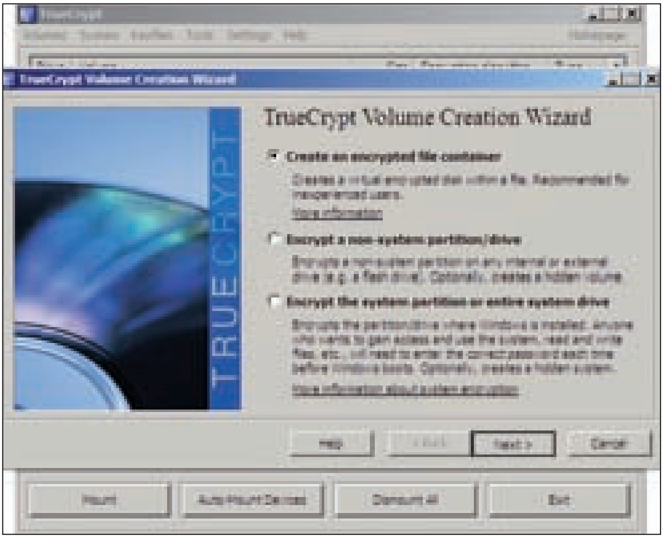
Now the database is opened up, and you can go about adding the relevant details. Add in the website, the account information, and the login details. Enable auto-type for the frequently used entries. KeyPass is portable, so you can take these settings with you when you move between computers. When you enable Auto-type, a warning will pop up that Auto-type will not run on all windows. Auto-type just does not work in some very obscure scenarios, such as when a user is using a text based browser, or when using a command line interface. However it is unlikely that a lay user will run into such applications.

While enabling Auto-type, there is a check box for enabling obfuscation. Obfuscation is the feature that bamboozles keyloggers. Targeted programs can be written to bypass the obfuscation, but these are rare. When you enable obfuscation, a prompt will appear that warns you that obfuscation does not work all the time, this is for the command-line scenario, so you can ignore it.

5.3 Hide and password protect data

TrueCrypt is an excellent free encryption software, that securely hides away data. The data is encrypted using strong encryption algorithms called ciphers. If anyone gains access to the data, they will not be able to open, read or write the data. For all appearance, it is just a garbage file, that is a file that takes up disc space without serving any useful purpose. One of the many approaches that TrueCrypt has to securely store data, is to create a virtual file container. This creates a virtual hard drive, then encrypts it. The entire drive is saved as a single file, which is something like an expanding image file. Once you give in the correct password, and a keyfile, if you choose to use one.

Once you have installed TrueCrypt, go to Volumes>Create New Volume. The TrueCrypt Volume Creation Wizard opens up. There are three choices available, choose the first one. This is “Create an encrypted file container”. The description suggests this for new and inexperienced users, because this option will not mess up your operating system, or any other drive if



TrueCrypt Volume Creation Wizard

● Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

○ Encrypt a non-system partition/drive

Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

○ Encrypt the system partition or entire system drive

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

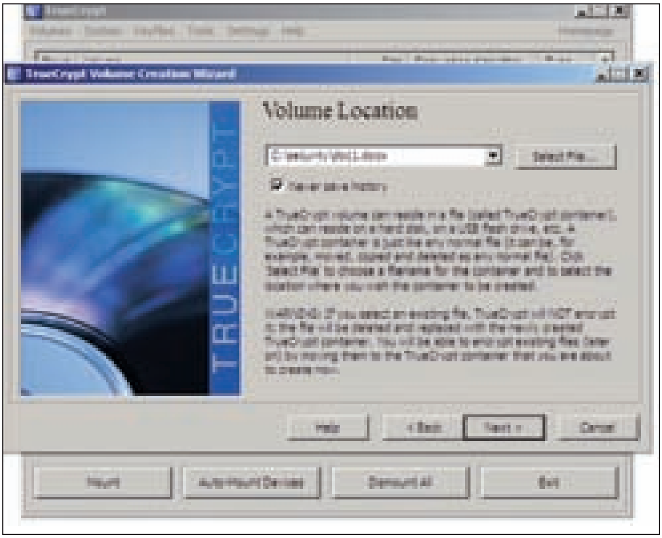
More information about system encryption

Creating a standard TrueCrypt volume

something goes wrong. Select this option, and click on Next.

There are two options available in the next step. The first option is a standard TrueCrypt volume, the second option is a hidden TrueCrypt volume. The standard TrueCrypt volume should be the choice for most users. The standard TrueCrypt volume is also hidden, and encrypted, but the hidden TrueCrypt volume offers another layer of inpenetrability. In case, for any reason, someone comes to know that you have hidden data in a virtual container, and you are forced to reveal the password and the passkey to the person, then the hidden TrueCrypt volume will come to your rescue. What this does is create two hidden volumes, a fake one and a real one. The user will have to convincingly hide sensitive looking data in the fake hidden volume, so that the user can show this data when forced. However, for most users, the standard TrueCrypt volume is good enough.

Click on Next. In this dialogue box, you will have to choose a file. You need a path for the file, but the prompt is designed in a slightly confusing way. You will have to navigate to a particular



☑ Never save history

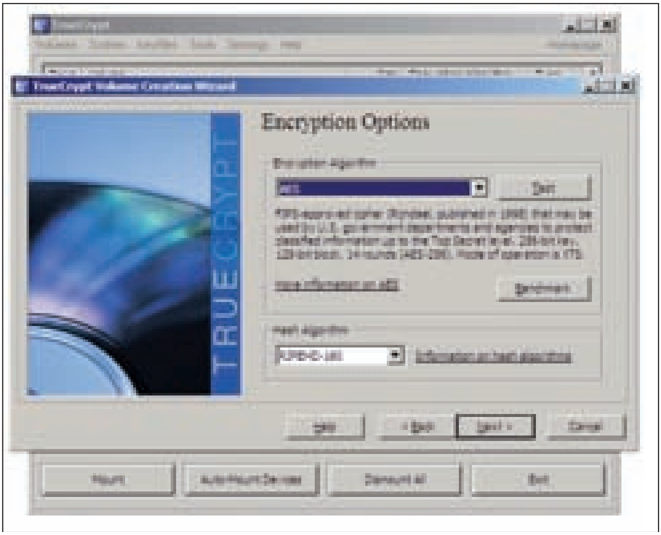
A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved, copied and deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

Selecting a file as the virtual container

file and select it. An easy way to do this is create a blank text file and select it. The encrypted volume can have any extension, so you can hide the file in plain sight, and people won't know what it is. Some extensions are prompted as being problematic, including .dll, .exe, .bat and a few other system related extensions. Even if you use these extensions, by and large, there should not be any major problems.

The next step is to select an encryption algorithm. This is known as a cipher. A cipher is used to encrypt and decrypt files. This process is related to the password and the keyfile, so another decrypter cannot decode the files if the password is not known. The encryption algorithms are very strong, and used by governments and the military worldwide. The AES is the encryption standard, serpant was a close contender to becoming the encryption standard, and twofish is based on blowfish, which was an old encryption standard. You can choose any of these encryption methods, or a combination of the two. AES is considered to be the best compromise between speed of



FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

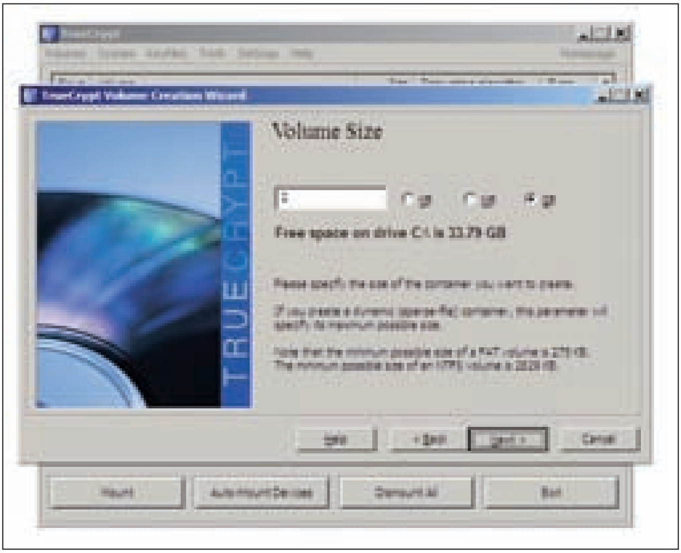
Choose an encryption algorithm

encryption/decryption and strength of the encryption.

The next step is to choose a size for the container. It is possible to choose a dynamically expanding container. This means that the size of the container increases as and when you put data into it. The more secure, and less suspicious way is to create a fixed size container. The prompt allows you to specify the size of the container in KB, MB or GB. Note that you can move the container to other locations later on, just copy and paste the file. For now, select a size and click on next.

The next step is to create a password. A password of around ten characters should be good enough for any lay user. Users can additionally, choose to add keyfiles. A keyfile can be any file that the user wants. Once generated or selected, a keyfile is necessary for opening the document. You can choose any file as the keyfile, or create your own by using an image file or a text file. Without the keyfile, you wont be able to access your data, so keep it carefully.

The next step is to format the volume. This allocates a virtual file system for the volume you are creating, without



Volume Size

Free space on drive C:\ is 33.79 GB

Please specify the size of the container you want to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.

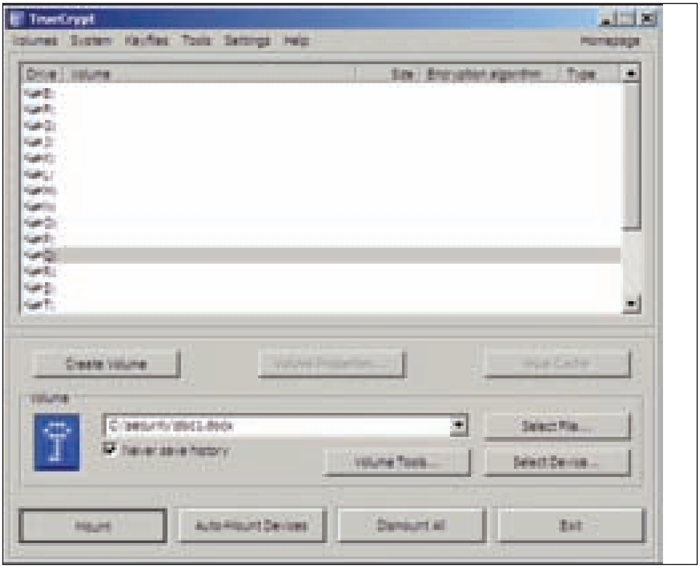
Note that the minimum possible size of a FAT volume is 275 KB. The minimum possible size of an NTFS volume is 2829 KB.

Selecting a size for the virtual container

affecting the file system of the volume you are storing the file on. This just dictates the behaviour of the location within the virtual drive, where your data is going to be stored. The location has to be formatted in accordance with the selected drive format, so this will take some time.

That is it, your volume will now be created. To create another virtual volume, click on next. Otherwise, click on Exit. Now, TrueCrypt is necessary to mount the volume. What mounting the volume does is emulate the file as a drive partition on your system. Select one of the free mount points available in the main menu. These will be a list of the alphabets not already used by drives on your system. Then, select the file that you used as the container for the virtual volume, and click on Mount. You will be prompted for the password and the keyfile, if you chose to use one. Once these are entered, your encrypted and hidden volume is mounted as a drive on your system, and you can copy and paste data in and out of it, or work on it directly.

You can also carry around the file, along with TrueCrypt,

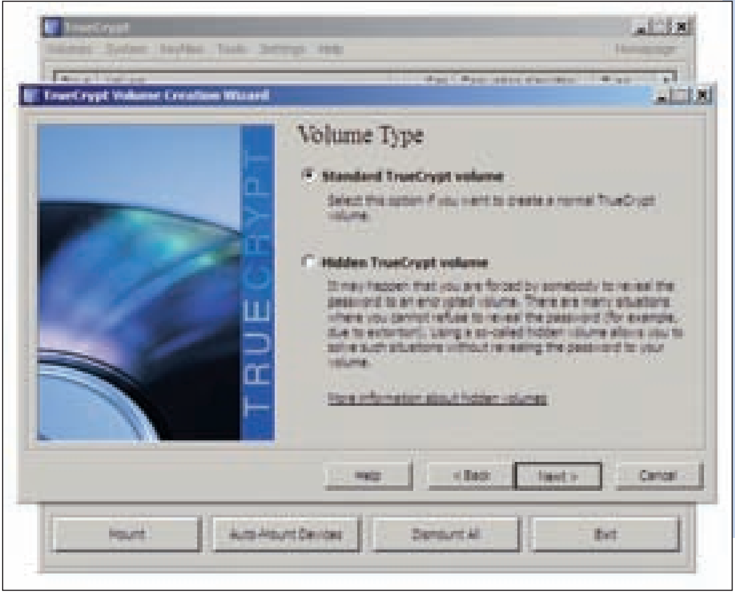


Mounting a volume

and use the same container on multiple locations. Save the container on a portable device, and you have a portable encrypted location for storing your data securely.

5.4 Password protect drive access

TrueCrypt can also be used to password protect drive access. This can either be portable drives, or the drives on a machine. We'll be first detailing how to completely encrypt a portable drive. The drive will detect on all systems, but will display as being unformatted. To read or write in the drive, you will have to mount it on another mount point in the system, then enter the password. That is, if the portable drive is allocated the drive letter G by the system, you will have to mount it using TrueCrypt to drive letter H to be able to write and read from it. Before encrypting the drive, copy all the data to another location. Although TrueCrypt can keep the data on the drive, this is a longer process. The data is moved around, the drive is



Volume Type

● Standard TrueCrypt volume

Select this option if you want to create a normal TrueCrypt volume.

○ Hidden TrueCrypt volume

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

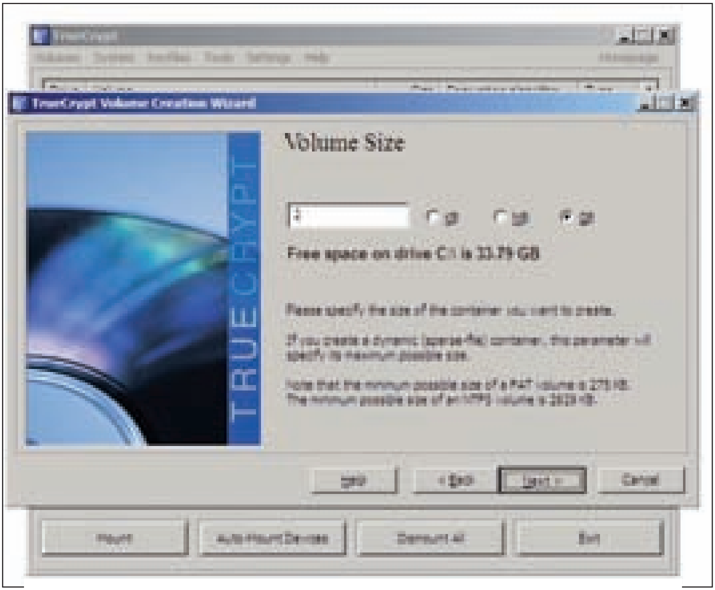
More information about hidden volumes

Encrypting a non-system partition

encrypted, and the data is moved back in. This is faster if the user does it. We will be showing a method that deletes all the data in the drive, as it is considerably faster and more practical. Go to Volumes>Create New Volume in TrueCrypt. Select the second option, Encrypt a non system partition/drive. Then click on Next.

Select the Standard TrueCrypt volume as the volume type. Then select a partition or device. In this step, you can either choose an external drive, or a drive where the operating system you are running is not located. On most systems, this means everything but the C drive is ok to go. Here, we are encrypting a thumb drive.

Click on Next. Then select a creation Mode. To save time and resources, choose Create Encrypted volume and format it. Then click on next. The encrypt partition in place should be used only when you have nowhere else to transfer the data to. In that case, it's a good idea to leave the operation overnight, and is a little risky as you have to ensure that the power is supplied



Volume Size

Free space on drive C:\ is 33.79 GB

Please specify the size of the container you want to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.

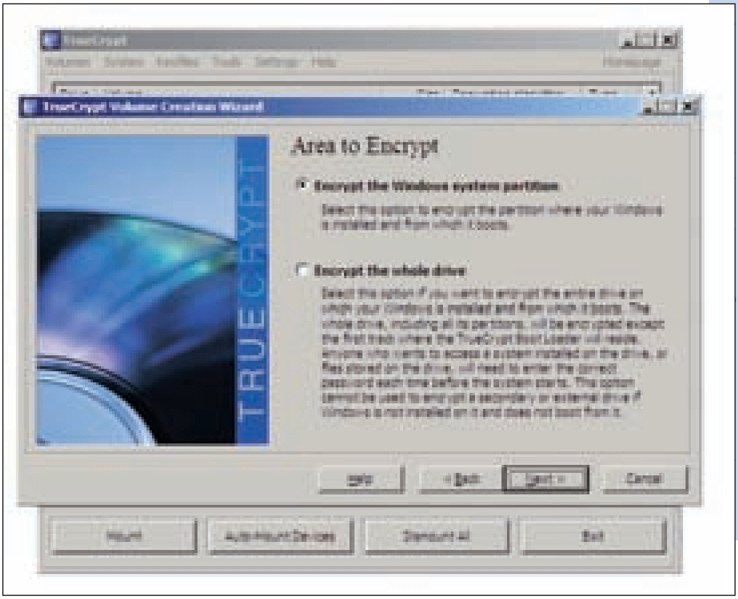
Note that the minimum possible size of a FAT volume is 275 KB. The minimum possible size of an NTFS volume is 2829 KB.

Create encrypted volume and format it

throughout the operation.

Next, select an encryption algorithm, and click next. You will be prompted about the imminent loss of all data on your drive. Agree, and continue. That is it, whether this is an external drive, or a non-system partition, you will have to mount it using the password and TrueCrypt, before it shows up in the list of drives on the system.

TrueCrypt can also be used to encrypt a system volume, which is the partition of the hard drive where the operating system is located. Doing this is a little risky, because if you forget the password, you won't be able to boot up your machine. Go to Volume>Create New Volume, and select the third option, which is "Encrypt the system partition or entire system drive". Choose "Normal" as against "Hidden". The "Hidden" option creates a fake encrypted Operating System. There will be two hidden and encrypted Operating System on the system, and you can reveal one of these under force.



Area to Encrypt

● Encrypt the Windows system partition

Select this option to encrypt the partition where your Windows is installed and from which it boots.

○ Encrypt the whole drive

Select this option if you want to encrypt the entire drive on which your Windows is installed and from which it boots. The whole drive, including all its partitions, will be encrypted except the first track where the TrueCrypt Boot Loader will reside. Anyone who wants to access a system installed on the drive, or files stored on the drive, will need to enter the correct password each time before the system starts. This option cannot be used to encrypt a secondary or external drive if Windows is not installed on it and does not boot from it.

Choosing a partition or a drive

Now there are two options. The first option allows you to encrypt just the partition of the hard drive where the operating system is located. The second option allows you to encrypt not just the partition where the operating system is located, but all the partitions on the drive where the operating system is located. There is no option to encrypt all the drives in the hard disk, because this can be done through the Operating System later on. TrueCrypt does this by installing a small bootloader in the hard drive, which requires the password to be entered before the Operating System boots up. Click on Next.

The next Window gives users a choice on encrypting the host protected area of the Operating System. This is usually where the backup data is located, or some such functionality in Laptops and on some Desktops. The safest option here is to select No.

The next screen is for advanced users. Most users can select single boot. However, if your machine has more than one operating system installed, select Multi-boot. TrueCrypt is cross platform, so the same method can be used from a Linux Operating System to encrypt and password protect a Windows installation on the same machine. Note that, in case of multi-boot, the other Operating System need not be located on the same hard drive as the one being encrypted, this option is just so that the TrueCrypt bootloader is configured correctly.

The next step is to choose the encryption algorithm. Choose an cipher, and click on Next. Then, key in a password. If you choose to use a keyfile at this point of time, the keyfile will have to be selected before system load from an external device. This means that every time the Operating System has to be booted, there has to be a USB drive plugged in to the system. This is very secure, but if you lose the keyfile, you will lose access to your data as well.

The next step generates encryption keys using random data. Just move the mouse randomly for some time, and click on next. The next window allows you to create a rescue disc in case you lose your keyfile. This operation basically allows you to restore the system to the current state. This is necessary in case your keyfile gets corrupt, the bootloader gets corrupt, or the Windows installation becomes unusable or infected by malware. The rescue disc is an iso image that must be burned on, which is a bootable disk. Burn the iso image before proceeding with the encryption. Don't burn the image on the DVD itself, but burn the files inside the iso, that is open the iso file using a DVD burning software, and proceed.

You will have to burn the disc, put it in the tray, and click on `Customize the bootloader.` Click on Next.

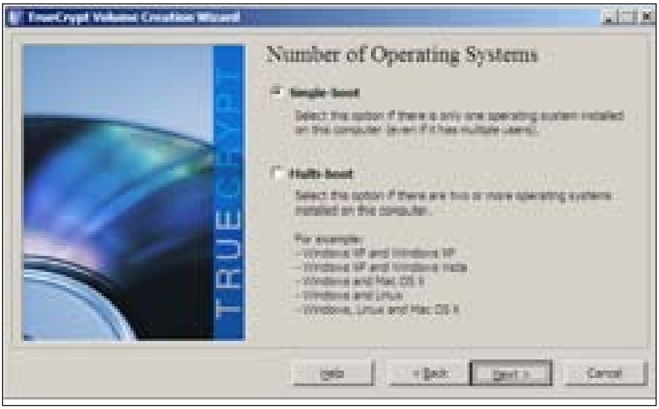
You get to customize the bootloader now. Enter some text for the password prompt. This can be anything that you prefer. Click on Next, and the encryption process starts. This will take some time. The next time you boot the operating system, you will be prompted for a password.

5.5 Securely format drives

Sometimes, it is important to delete data. This can range from sensitive documents to keyfiles. The ability to erase securely is more important when using public computers, or shared computers. Also, if you are selling away old hard disks, it is very important to securely format such drives. There have been many cases of data thefts recovering sensitive materials from hard drives sold off in auctions. Deleting the data from the recycle bin is not enough, or using shift+delete does not really delete the data. What these operations do is remove the index of the particular files from the index. A file recovery tool, as demonstrated above, can recover files from such drives. The data will remain in the hard drive for long periods of time, especially if the files are small in size.

Software for securely deleting data are available. These software delete the file from the index, as well as replace the actual data on the drive with pseudorandom data. The physical location of the data on the disk is overwritten, so the chances of recovering the data is greatly reduced. We will be showing how to use two free programs for deleting data, but there are more available. These are both freeware. FreeCommander is an alternative to Windows Explorer, and has a number of extra features. FreeCommander securely deletes data quickly and easily. Eraser is another application, and it can be configured to overwrite the data many times over. Eraser is the more secure and robust file shredding application, but is also far more time consuming because of the numerous overwrite runs required.

Free Commander is a free file browser that makes exploring the file system easier. Folders show up with sizes, and there is



TrueCrypt Volume Creation Wizard

Number of Operating Systems

● Single-boot

Select this option if there is only one operating system installed on this computer (even if it has multiple users).

○ Multi-boot

Select this option if there are two or more operating systems installed on this computer.

For example:
- Windows XP and Windows XP
- Windows XP and Windows Vista
- Windows and Mac OS X
- Windows and Linux
- Windows, Linux and Mac OS X

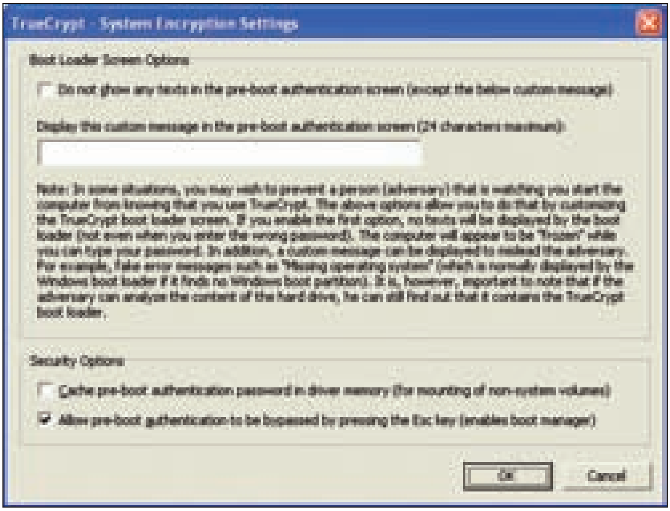
Single or Multi boot

a dual pane interface that makes moving data around a breeze. To securely delete data, select the files or folders, then go to File>Wipe.

Free Commander offers upto 10 overwrite runs. Each "run" involves rewriting the area where the data was stored with random data. The more the runs, the more irrecoverable the data becomes. However, if you have deleted data, without wiping it, then it can be recoverable by a file recovery software. Free Commander has no function to erase the empty hard disk space, and rewrite the empty information.

This is where Eraser steps in. Eraser is a deceptively simple looking program. Eraser can securely delete the data even in the free space section of the hard drive, where data exists, but is not indexed. Go to File and add tasks to add the parts of the hard disk that has to be erased. The user can add empty hard disk space, specific folders, or individual files. Each operation is called a task, and any number of tasks can be added to a list known as the task list. Eraser goes through the task list, erasing the identified data one at a time.

At each instance of an erasing operation, there are a whole range of secure deletion options available to the user. There are



TrueCrypt - System Encryption Settings

Boot Loader Screen Options

□ Do not show any texts in the pre-boot authentication screen (except the below custom message)

Display this custom message in the pre-boot authentication screen (24 characters maximum):

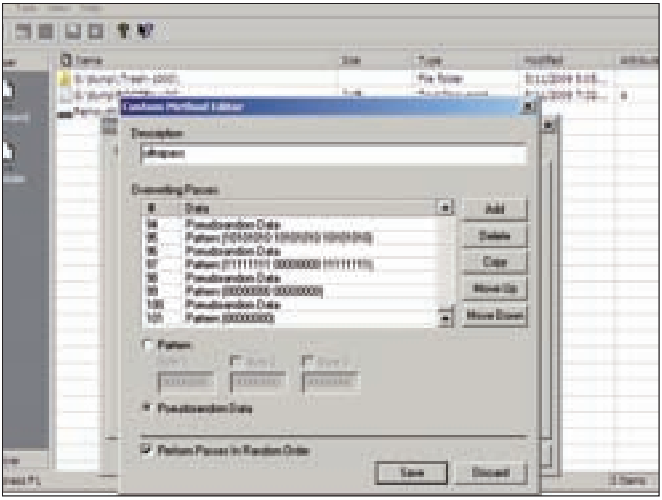
Note: In some situations, you may wish to prevent a person (adversary) that is watching you start the computer from knowing that you use TrueCrypt. The above options allow you to do that by customizing the TrueCrypt boot loader screen. If you enable the first option, no texts will be displayed by the boot loader (not even when you enter the wrong password). The computer will appear to be "frozen" while you can type your password. In addition, a custom message can be displayed to mislead the adversary. For example, fake error messages such as "Missing operating system" (which is normally displayed by the Windows boot loader if it finds no Windows boot partition). It is, however, important to note that if the adversary can analyze the content of the hard drive, he can still find out that it contains the TrueCrypt boot loader.

Security Options

□ Cache pre-boot authentication password in driver memory (for mounting of non-system volumes)

☑ Allow pre-boot authentication to be bypassed by pressing the Esc key (enables boot manager)

Customize the bootloader



Creating a custom pass pattern

a few default patterns in which the erasing occurs, but this can be entirely tweaked by the user. The most secure default pattern offered by the program is the Gatmunn method, which involves thirty five passes.

This is more than anyone really requires. However, to give yourself the illusion of extra security, and more importantly, peace of mind, you can choose to create your own erase/overwrite patterns. Click on new to create your own pattern. You can specify an unlimited number of passes, and define what kind of data is used to overwrite the file or empty space in each of these passes. A pattern overwrite uses a specified pattern, and the pseudorandom data overwrites with random characters. We specified an operation which implements 101 passes.

Note here, that the more passes you specify, the more is the time taken. Overwriting files and folders is a relatively fast operation, compared to rewriting all the empty space in a hard disk. Even a 10 passes operation will take a long time when it comes to clearing hard disks with a lot of empty space. Also note that two or more identical passes, following the same pattern (say all zeroes) is the same as one pass with that pattern. Either alternate the pattern, or sandwich patterns between two pseudorandom data passes. Deleting all the existing data in the hard drive, then erasing all the empty space using Eraser will securely delete all the data on your hard drive. Now even specialists cannot recover the data easily from your hard disk. It is safe to sell or dispose hard disks only after you have securely deleted all the data on the drive.

6 Mobile phones

In this wireless and busy world, mobile phones can't be left far behind in the war of viruses and counter measures. Gone are the days when mobile were used only for placing calls and messaging. Todays' mobile phones are used to do everything from calling, messaging, blogging, browsing, transferring files by means of Bluetooth and MMS. With cellular mobility and handhelds evolving by the months, and their increasing resemblance to computing devices, they are getting increasingly vulnerable to attacks and infringement of our privacy.

Every time you connect your phone to the computer to transfer images or share your contact list, you are just opening up yourself to a host of malicious coding out there aimed solely at causing harm to your device. Also, the next time you are in a public place and are sharing files over Bluetooth make sure you pair up with trustworthy devices. This could save you a lot of pain in the literal sense. Read on more to find out remedies in case you happen to be infected. Even if you aren't, you'll get to know of some helpful remedial steps to prevent such events.

6.1 Password protect phone access

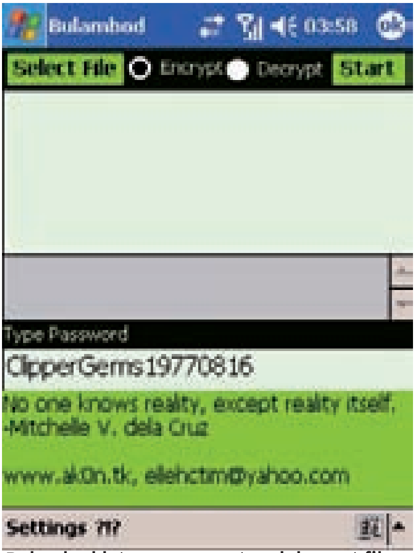
Password protection is not a new feature in cellular phones. This is among those rarely used functions available in most handsets. All phones have this one function to set a password to your phone to prevent misuse. However, we do warn that you still need to monitor your phone and not leave it to unauthorised use. While going through the functions in your phone, you'll come across two security codes – PIN and PIN2. These are two codes which are generally 4 digits wide, but can go up to 8 digits. PIN is used to prevent unauthorised access to your cell phone. Normally, most OEMs set these to default values of 1234 and 12345, respectively. You or the handset user would be prompted to key in the PIN on accessing keypad.

Similarly, in order to access the priority numbers in the phone, there is another PIN2 that you need to key in. As a protective measure, the phone gives you just three chances at entering the correct PIN. So be sure, don't take your password lightly. If you don't get the code right on the third try, the subscriber identity module (SIM) card gets locked. Once your SIM card is locked, you need to contact your cellular operator and request a PIN unlocking key (PUK). Your operator would provide this code after you verify your identification and provide them with your international mobile subscriber identity (IMSI) number. You can get your IMSI by referring to your SIM card. It's the 15-digit number printed on your SIM.

By taking this single precautionary step, you would save any fidgety and inquisitive person from getting hold of your personal information. For increased security, you can install third-party applications to prevent unauthorised access to your phone. However the choice depends on how critical the information on your phone is. Else, increasing the number of applications on your handset would just eat into the processor causing a slowdown in its operation. Practically, one, or at the most two levels of security is more than sufficient. Depending on what you want to keep away, you can use either of the solutions mentioned in the following sections.

6.2 Hide photos and videos

Our phones give insights into our deepest secrets. It has our contacts in addition to our personal messages. With the advent of cameras and memory cards in mobile phones, it also has our personal and intimate moments captured. This not only requires us to be more responsible for ourselves, but for all those who stay captured on our handsets. This further increases the need to ensure the photos and



Type Password

ClipperGems19770816

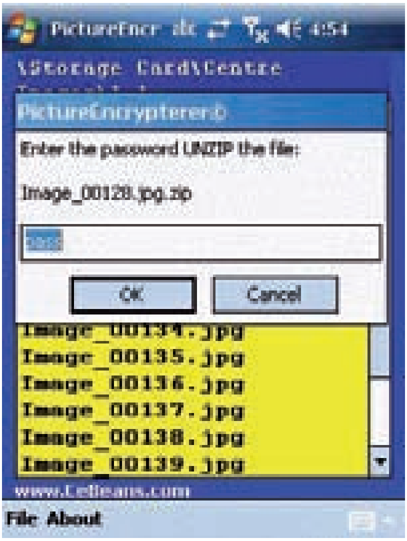
No one knows reality, except reality itself, -Mitchelle V. dela Cruz

www.akOn.tk, ellehctim@yahoo.com

Bulambod lets you encrypt and decrypt files, so that only you have access videos that we have captured and stored on our mobile phones don't fall into the wrong hands.

Multimedia content is in no way different. One way of hiding these files from external access is by disabling their ability to be played by the phone's multimedia player. The easiest way to do this is to remove the file associations by renaming the file on the memory stick. This way, although you still have your images and videos with you, any unknown anonymous person cannot view them while you are away.

Another promising application is Bulambod. The creator claims it is an unbreakable cipher. In cryptography terminologies, a cipher is an algorithm that performs encryption and decryption operations on any given information or data.



Enter the password UNZIP the file:

Image_00128.jpg.zip

Image_00134.jpg
Image_00135.jpg
Image_00136.jpg
Image_00137.jpg
Image_00138.jpg
Image_00139.jpg

With PictureEncrypter you can assign passwords to your pictures

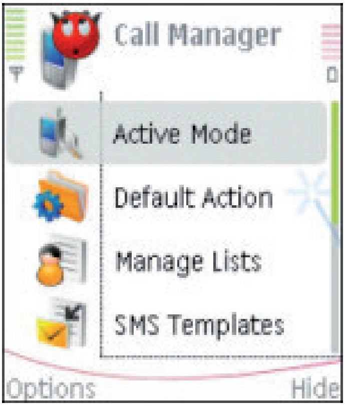
Simply put, a cipher is the code used to encode and then eventually decode the message. All you need to do is select a file that you need to encrypt, enter your password and Bulambod will do the rest. Decryption is also easy. There is no limit on the length of the password that you can use and so it is difficult to crack.

You can download this application at **http://handheld.softpedia.com/get/Security/Encryption/Bulambod-70808.shtml**.

If all you want to do is encrypt your photos, you can also use PictureEncrypter.

Download PictureEncrypter at **http://handheld.softpedia.com/get/Security/Encryption/PictureEncrypterer-61052.shtml**. This application lets you ZIP your images and assign a password to it. To view your image, all you need to do is type the password and it will let you zoom into your image.

6.3 Hide and password protect access to messages



Take control of your call and message logs with Private Call and SMS guard

A mobile phone is meant for placing voice calls and messaging. With these two functions secure, you can be assured that your phone cannot be misused. For this, you can use Private Call and SMS guard. You can find this application at **http://www.getjar.com/products/7250/PrivateCallandSmsGuard**.

This application gives you the best of most call and SMS applications. It lets you personalise your phone by assigning rules to calls. You can individually set rules to accept or reject calls your contacts. This way you don't have to bother of whose call to accept and whose to reject. You only receive calls from people you are comfortable with! It also lets you set up a blacklist of numbers you don't wish to receive calls from.

Similar to calls, it also lets you set rules for messages. You can create a blacklist of numbers. Any message from a number on this list is automatically blocked.

6.4 Hide contact list

These days, mobile phones are indispensable companions. We find it difficult to do away with them. Nevertheless, it holds personal details and contacts to such an extent that it deserves the attention it gets from us. In fact, there's software aimed at protecting all the information in there.

On such application is Hidden Contacts by Tektronic SRL. You can download this application at **http://tektronic.ro/productdet.aspx?prodid=12**. With this application loaded, you can assign a password to select contacts on your list. For example, if you have some critical contacts that you wish to keep as a closely guarded secret, this application is for you. Not only does it hide the contact and other details in the list, it also sends the messages directly to the contact without having the message stored in the default sent items folder of your phone.

Additionally this application lets you lock the call log function of the phone. Not only will no one else know what you messaged your secret contacts, they won't even know if you called them. This ensures you and your contact of privacy.

6.5 Anti-virus for mobile devices

The rules for virus protection are more or less similar to those that hold true for PCs. Popular PC anti virus names also have solutions for mobile phones. Among them the most popular are F-Secure. You can access this at **mobile.f-secure.com**. Once you click on this link, you need to select the phone you use and then download the appropriate file. You will find the experience familiar with it downloading the virus database the first time.

F-Secure is an all-in-one suite and serves as an anti-theft application, anti-spyware and firewall in addition to being an anti virus. Click on the link that says try on the bottom right of the home page and you will be asked to register yourself. Fill in your name, country and email address. That is all the information they require of you. A download link is promptly sent to your email address. F-Secure also lets you run a real-time scan of your mobile. If it finds a virus in real time, it will prompt you. You can choose between viewing the file or deleting it.

Another popular mobile anti-virus is Kaspersky Labs' mobile solutions. You can download the application at **www.kaspersky.com/mobile_downloads**.

6.6 Disable password saving on WAP and GPRS

Similar to browsing on a public computer, the same holds true for your mobile phone. It is definitely not difficult for someone to gain physical access to your handset while you are away and get to your inbox simply because you saved passwords to reduce the need for some extra key pressing. When using your phone's browser for browsing or using any popular mobile browser such as Opera Mini, we are often tempted to save our password, as it makes it so convenient to browse. All you need to do is initialise the application and you are ready.

This also has a downside to it. Hence, we should be cautious and it is wise to enter your password each time you browse.

6.7 Encrypt messages

Blender xxTea edition

You can use for encrypting your messages and any other information is Blender. You can download Blender at **http://handheld.softpedia.com/progDownload/Blender-XXTea-Edition-Download-70031.html**. With Blender, all you need to do is store your messages like you normally do.

All you need to do is store your data normally in the places you do. So be it your messages, Notes, tasks or Contacts, you can encrypt them using Blender. Send this encrypted data over email or send it as a file or your recipient as a message who can decrypt it using Blender so that only the two of you can understand the message. Since Blender can be used even on a web page, you do not need your mobile phone to decode or read the messages. All that is needed is the same cipher.

However, with Blender you cannot encrypt short messages such as short PIN numbers because Blender does not encrypt messages with a character length of 4 characters of less.

6.8 Filter spam messages

As if spam in our emails were not enough, that we needed spam on our mobiles too! But then, it's all about business and everyone out there wants to earn a quick buck. The result – we, the victims of spam. It's high time we took control of the situation. We could also help our friends and family out of the menace.

One application that is effective in arresting SMS spam is SMS Spam Manager. You can access this application at **http://www.webgate.bg/products/ssm/**. Once you download SMS Spam Manager, you need to configure it by setting the filters for blocking spam. There are six rules for this. This way you are able to filter all your incoming text messages. The first three rules are general – Accept all, block all, and Accept phonebook only.

Accordingly, all messages are allowed when you select Accept all. In this case, the filters are inactive and they do not monitor the messages you receive. In case of Block all, again it is similar. Spam Manager will not monitor the messages in any way, but rather block all messages. The safest filter, however is the third case where only messages from contacts in your Phonebook are allowed to pass through. This way you are assured that you receive messages only from known people.

The remaining three filters in SMS Spam Manager are worth noting, because these are what effectively fight the spam menace. You can block messages on the basis of telephone number, prefix number or text match. This is really effective. No longer would those messages from those short code special numbers go undetected. All we used to see was some number as 45678 and there was nothing we could do. With Spam Manager, this number is detected and automatically blocked.

However, there is a catch to it. For example, your cellular operator keeps sending you offers for services in astrology and also those love and beauty tips. You're probably disgusted with them, but you don't want to miss out on your bill status. All these messages probably originate at the same number. Therefore, blocking out that number wouldn't be a wise decision after all. All you need to do is type in the phrase that typically appears in the spam messages. So, "know what your stars say" or "Special love tips" or "lose 5 kgs in a week" could reduce your agony drastically, if not put an end to it!

Finally, nothing is lost. Similar to a spam folder in your mailbox where you can occasionally go and check if you have lost any mail, you can check to see if any message has been wrongly filtered out as spam and restore them to your inbox.

6.9 Theft protection

Phone theft is rising by the day. We have heard of all kinds of technologies being implemented by cellular manufacturers these days to ensure that you would be able to recover your handset in the event of theft. But what if your handset is not equipped with such technology? You should not be left behind. Phone Guardian was aimed at such users. You can download Phone Guardian v3.0 at **http://www.filecluster.com/downloads/Phone-Guardian.html**. This application works by auto locking your phone in case it is stolen. To do this, you need to send a lock SMS.

Phone Guardian decodes the message and understands that your phone is not in your possession any more and automatically locks your phone. This prevents abuse of your personal information. Whoever recovers the phone will only be able to use any function of the phone unless they know the correct password. So beware, do not commit the blunder of forgetting your password – you will not be able to uninstall Phone Guardian after it gets locked.

In the latest version of Phone Guardian, there are so new features that further increase security. It has a new GPS tracking option, whereby you can remotely track your phone by controlling the GPS module by sending text messages to your phone.

Xpress alarm

Another application aimed at preventing mobile phone theft is Xpress alarm. With this, all you need to do is keep your phone in your pocket. The moment your phone is outside the pocket, it sounds an alarm. You can dowload Xpress alarm at **http://handheld.softpedia.com/progDownload/XpressAlarm-Download-77817.html**.

Despite all the applications available here, nothing is more effective than being responsible. Taking ownership of your phone comes before everything else. With every development in technology, there are counter measures being developed all the time. For every password encrypter, there is a decrypter being developed.

Also, we would like to stress on the need to use original software. In the applications we have mentioned, some do provide advanced functionalities on registering and paying a fee. If you really need these functions, you should consider purchasing the original software rather than using pirated versions or opting for a cracked version. On second thoughts, we should not feel the pinch if our mobile phones are stolen if we use pirated software – that is theft after all!

Finally, by staying safe, you just don't need so many precautionary measures. Practice self monitoring over the files you store on your phone. Take adequate precautionary measures while transferring file to and fro your computer. A simple step as showing your hidden files and folders would tell you of unseen infections residing on your memory. You can then delete them before they create havoc. Ensure you transfer files with known and trustworthy people only. This way you can at least be sure the ones you are pairing up with don't have unfriendly motives.